VŠB – Technická univerzita Ostrava
Fakulta elektrotechniky a informatiky
Katedra telekomunikační techniky

Virtuální privátní sítě s využitím firewallů ASA

Virtual Private Networks Using ASA Firewalls

2017 **Bc. Jaroslav Fidermák**

VŠB - Technická univerzita Ostrava
Fakulta elektrotechniky a informatiky
Katedra telekomunikační techniky

Zadání diplomové práce

Student: **Bc. Jaroslav Fidermák**

Studijní program: N2647 Informační a komunikační technologie

Studijní obor: 2601T013 Telekomunikační technika

Téma: Virtuální privátní sítě s využitím firewallů ASA
Virtual Private Networks Using ASA Firewalls

Jazyk vypracování: čeština

Zásady pro vypracování:

Cílem diplomové práce je návrh, realizace a testování různých řešení virtuálních privátních sítí v laboratorním prostředí s využitím firewallů ASA.

Osnova práce:
1. Popište různá řešení sítí VPN.
2. Navrhněte a v laboratorních podmínkách realizujte alespoň tři druhy sítí VPN na firewallech ASA. Ověřte funkčnost navržených řešení.
3. Srovnejte jednotlivá řešení. Zhodnoťte výhody a nevýhody jejich použití.
4. Popište a prakticky otestujte odlišnosti při implementaci sítí VPN na firewalech ASA v porovnání se směrovači Cisco řady 2900.

Seznam doporučené odborné literatury:

[1] DEAL, Richard. *The Complete Cisco VPN Configuration Guide.* Indianapolis: Cisco Press, 2006. ISBN 1-58705-204-0.
[2] FRAHIM, Jazib a Omar SANTOS. *Cisco ASA: all-in-one firewall, IPS, and VPN adaptive security appliance.* 3rd ed. Indianapolis: Cisco Press, 2014. ISBN 9781587143076.

Formální náležitosti a rozsah diplomové práce stanoví pokyny pro vypracování zveřejněné na webových stránkách fakulty.

Vedoucí diplomové práce: **Ing. Petr Machník, Ph.D.**

Datum zadání: 01.09.2016

Datum odevzdání: 28.04.2017

doc. Ing. Miroslav Vozňák, Ph.D.
vedoucí katedry

VYSOKÁ ŠKOLA BÁŇSKÁ-TECHNICKÁ UNIVERZITA * Fakulta elektrotechniky a informatiky * 1D16 * OSTRAVA *

prof. RNDr. Václav Snášel, CSc.
děkan fakulty

Prohlášení studenta

Prohlašuji, že jsem tuto bakalářskou/diplomovou práci vypracoval samostatně. Uvedl jsem všechny literární prameny a publikace, ze kterých jsem čerpal.

V Ostravě dne: *26. dubna 2017*

.....
podpis studenta

Poďakovanie

Rád by som poďakoval Ing. Petrovi Machníkovi Ph.D. za odbornou pomoc a konzultácie pri vytváraní tejto diplomovej práce.

podpis zástupce

Abstrakt

Témou diplomovej práce bolo popísať rôzne druhy VPN, ktoré sú používané a podporované zariadením Cisco ASA 5505. V prvej časti sú popísané bezpečnostné metódy používané na zabezpečenie VPN. Takisto sú v tejto kapitole podrobne vysvetlené jednotlivé technológie VPN ako IPSec, SSL a L2TP/IPSec. V ďalších kapitolách je pre každú popísanú VPN technológiu navrhnuté zapojenie, ktoré je prakticky zrealizované na firewalle Cisco ASA 5505 a pripravené na použitie v reálnej sieti.

VPN sa používajú aj na smerovačoch Cisco. V diplomovej práci budú už spomenuté VPN technológie prakticky otestované aj na smerovači Cisco 2901 a následne bude porovnávaná implementácia a funkčnosť jednotlivých riešení.

Kľúčové slova

Virtuálna privátna sieť, Cisco ASA 5505, Cisco 2901 IPSec, SSL VPN, L2TP/IPSec VPN

Abstract

The subject of the master thesis was to describe different types of VPN, which are used and supported by Cisco ASA 5505 device. In first part there are described safety methods used to secure VPN. There is also explained each VPN technology as IPSec, SSL, and L2TP/IPSec in detail in this chapter. In other chapters there is designed topology for each described VPN technology, which are practically implemented on the firewall Cisco ASA 5505 and ready to use in real network.

VPN are used on Cisco routers, too. In this Master thesis, mentioned VPN technologies will be practically tested also on the Cisco router 2901, and subsequently implementation and functionality of different solutions will be compared.

Key words

Virtual private network, Cisco ASA 5505, Cisco 2901, IPSec, SSL VPN, L2TP/IPSec VPN

Obsah

Zoznam použitých skratiek

Skratka	Anglicky význam	Slovenský význam
AAA	Authentication authorization accounting	Autentifikácia autorizácia účtovanie
AES	Advanced Encryption Standard	Štandard pokročilého šifrovania
AH	Authentication Header	Autentizačná hlavička
ASA	Adaptive security apliance	Adaptívne bezpečnostné zariadenie
CA	Certification Authority	Certifikační autorita
DES	Data Encryption Standard	Štandardné šifrovanie dát
DH	Diffie–Hellman	Diffie–Hellman
DHCP	Dynamic Host Configuration Protocol	Dynamická konfigurácia hostiteľského kľúča
DNS	Dynamic Name Server	Dynamický názov server
DOS	Denial of Service	Útok odmietnutia služby
DTLS	Datagram Transport Layer Security	Datagramová bezpečnosť transportnej vrstvy
ESP	Keyed-hash Message Authentication Code	Kľúčový hašovací autentizačný kód správy
HMAC	Keyed-hash Message Authentication Code	Kľúčový hašovací autentizačný kód správy
ICMP	Internet Control Message Protoco	Protokol riadiacich správ Internetu
IKE	Internet Key Exchange	Výmena kľúčov po internete
IP	Internet Protocol	Protokol Internetu
IPSec	Internet Protocol Security	Bezpečnostný Internetový protokol
ISP	Internet Service Provider	Poskytovateľ služieb Internetu
L2F	Layer 2 Forwarding	Poslanie z druhej vrstvy
L2TP	Layer 2 Tunneling Protocol	Tunelovací protokol druhej vrstvy
LAC	L2TP Access Concentrator	L2TP prístupový koncentrátor
LAN	Local Area Network	Lokálna sieť
LNS	L2TP Network Server	L2TP sieťový server
MPPE	Microsoft Point-to-Point Encryption	Šifrovanie bod - bod
NAS	Network Access Server	Sieťový prístupový server
NAT	Network Address Translation	Sieťový preklad adries
OTP	One-time password	Jednorazové heslo
PKI	Public Key Infrastructure	Štruktúra verejných kľúčov
PPP	Point-to-Point Protocol	Protokol dvojbodového spojenia
PPTP	Point-to-Point Tunneling Protocol	Protokol dvojbodového tunelovacieho spojenia

PRF	Pseudo-Random Function	Pesudo-náhodné číslo
RA	Remote access	Vzdialený prístup
RRI	Reverse Route Injection	reverzné vloženie statickej cesty
RSA	Rivest-Shamir-Adleman	Asymetrické šifrovanie
SA	Security Associations	Bezpečnostný asociácia
SAD	Security Association Database	Bezpečnostná asociácia databáz
SPI	Security Parameter Index	Bezpečnostný parametrový index
SSH	Secure Shell	Zabezpečený Shell
SSL	Secure Sockets Layer	Vrstva bezpečných socketov
TCP	Transmission Control Protocol	Prenosový riadiaci protokol
TLS	Transport Layer Security	Bezpečnosť transportnej vrstvy
UDP	User Datagram Protocol	Užívateľský datagramový protokol
VLAN	Virtual Local Area Network	Virtuálna lokálna sieť
VPN	Virtual Private Network	Virtuálna privátna sieť

Zoznam obrázkov

Úvod

Bezpečnosť v dátovej komunikácií zohráva v dnešnej dobe dôležitú úlohu či už sa jedná o klienta využívajúceho služby napríklad vzdialeného servera alebo firmu, ktorá tieto služby poskytuje. Dôležitým krokom je zaistiť bezpečnosť dát, ktoré sú prenášané väčšinou nedôveryhodným prostredím, ktorým je Internet. Toto vieme zabezpečiť rôznymi bezpečnostnými prvkami ako je šifrovanie, ktorým zabezpečíme dôvernosť, hashovanie, ktorým zaistíme neporušenosť obsahu prenesenej správy, autentizácia, ktorá slúži na potvrdenie totožnosti a v neposlednom rade použitie certifikátu, ktorý slúži na potvrdenie totožnosti komunikujúcich strán. Spojením týchto parametrov vytvárame mechanizmus na zabezpečenie prenášaných dát vo virtuálnych privátnych sieťach.

Virtuálne privátne siete majú svoje využitie takmer v každej firme kedy potrebujeme bezpečne prepojiť sieť pobočiek, ktoré môžu byť každá v inom meste alebo pripojiť zamestnanca (ktorý pracuje z domu) do firemnej siete, aby mohol pristupovať k interným aplikáciám a serverom alebo popri cestovaní skontrolovať poštového klienta a podobne. Využitie nájdu aj v domácnostiach, ak napríklad používame dátové úložisko NAS a potrebujeme bezpečný prenos dát z ľubovoľného miesta, ktoré poskytuje pripojenie na Internet. VPN môžu slúžiť aj v prípade, že nechceme zverejniť miesto odkiaľ pristupujeme do Internetu alebo sa chceme vyhnúť odcudzeniu súkromných údajov prihlasovaním sa na verejnú wifi sieť a tak ďalej. Je naozaj veľa možnosti ako VPN využiť, no ich hlavnou myšlienkou je vytvoriť rýchle, bezpečné, stabilné a spoľahlivé spojenie klienta s privátnou sieťou a dvoch alebo viacerých pobočiek medzi sebou.

Cieľom diplomovej práce je popísať a priblížiť fungovanie odlišných virtuálnych privátnych sieti, pre každú z nich navrhnúť jednotlivé riešenia, prakticky ich otestovať na zariadeniach Cisco rady ASA a následne ich zhodnotiť a porovnať odlišnosti v implementácií s Cisco smerovačom rady 2900.

V prvej kapitole nájdeme teoretický popis bezpečnostných metód, ktoré sú využívane vo VPN, a rôzne druhy VPN. V druhej kapitole sú prakticky realizované tri odlišné druhy VPN na zariadení Cisco ASA, ide o IPSec vo verzií IKEv2, SSL VPN a L2TP/IPSec. V tretej kapitole sú porovnávané a zhodnotené jednotlivé druhy VPN. Posledná, štvrtá kapitola je zameraná na konfiguráciu rovnakých VPN ako v druhej kapitole s tým rozdielom, že sú konfigurované na zariadení Cisco rady 2900. Ďalej je v tejto kapitole porovnávaná konfigurácia a funkcionalita medzi zariadením Cisco rady ASA a Cisco rady 2900.

1 Popis rôznych riešení sieti VPN

Virtuálne privátne siete slúžia na prepojenie dvoch privátnych sieti alebo pripojenie klienta k firemnej sieti cez verejnú sieť (Internet) a to prostredníctvom zabezpečeného spojenia nazývaného tunel. Týmto nahradíme prenajaté linky, ktoré sú síce bezpečné, ale za to veľmi nákladné. Pomocou VPN vieme vytvoriť šifrovaný tunel a zabezpečiť autentizovaný a dôverný prenos dát. [3]

V tejto diplomovej práci sa budeme zaoberať virtuálnymi privátnymi sieťami, ktoré sú podporované zariadením Cisco ASA 5505.

1.1 Popis jednotlivých typov VPN

VPN siete môžeme rozdeliť do dvoch skupín z hľadiska prepojenia. Ide o Site-to-Site VPN, ktoré slúžia na prepojenie lokálnych sieti a Remote access VPN, ktoré slúžia na pripojenie klienta k lokálnej sieti.

Site-to-Site VPN

Ide o spojenie jednej alebo viacerých pobočiek (sieti). Ako VPN brány sa používajú sieťové zariadenia, napríklad firewall alebo router, ktoré nadväzujú medzi sebou VPN spojenia a zároveň rozbaľujú alebo zapuzdrujú pakety. Koncové zariadenia nepotrebujú software ako VPN klienta na nadviazanie spojenia. [3]

Remote Access VPN

Je typ VPN, pri ktorej sa do lokálnej siete pripojíme pomocou VPN koncentrátora, ktorý slúži ako brána. Pre spojenie s lokálnou sieťou musí klient poznať IP adresu VPN brány a parametre zabezpečenia alebo sa pripojí pomocou softwaru Cisco Anyconnect klient. RA VPN je výhodná pre telecommuterov, ktorý potrebujú nadviazať spojenie z rôznych miest a informácie potrebné na spojenie s VPN sa dynamicky menia. Najrozšírenejšia RA technológia je SSL VPN. [3]

1.2 Parametre zabezpečenia

Dôležitou súčasťou VPN je aj ich zabezpečenie a preto v tejto časti popíšeme metódy šifrovania, certifikáty a algoritmus na výmenu kľúčov.

Šifrovacie algoritmy

Šifrovanie je premena obyčajného textu do formy, ktorá robí pôvodný text nezrozumiteľným pre neoprávneného príjemcu, ktorý nie je držiteľom daného kľúča na dešifrovanie správy. Šifrovanie je založené na výmene kľúča (kľúčov), kedy nevadí, že útočník pozná náš algoritmus, pretože ak nepozná náš osobný kľuč nedokáže prečítať dáta. Dešifrovanie je opačný proces, to znamená, že transformujeme šifrované dáta späť do obyčajného textu. Kryptografické algoritmy môžeme rozdeliť na symetrické a asymetrické. [9]

Symetrické algoritmy

Sú založené na princípe, kedy obe komunikujúce strany poznajú a používajú tajný kľúč na šifrovanie a dešifrovanie správ. Hlavným problémom je zabezpečenie výmenného kľúča, bez toho, aby bol odchytený treťou stranou (útočníkom). [9]

Asymetrické algoritmy

Používajú dva samostatné kľúče na šifrovanie a dešifrovanie. Každý komunikujúci partner vlastní dva kľúče, jeden verejný a jeden privátny. Správa je zakódovaná verejným kľúčom, ktorý je zdieľaný so všetkými, ale iba partner , ktorý má privátny kľúč môže správu dekódovať. [9]

Certifikačná autorita

Ide o subjekt, ktorý vydáva digitálne certifikáty pre klientov, ktorí potrebujú zaistiť autenticitu zdroja a integritu dát. Certifikát je digitálne podpísaný verejným kľúčom a je viazaný k identite jeho držiteľa. [9]

Diffie-Hellman

Jedná sa o kryptografický algoritmus, ktorý zaisťuje bezpečnú výmenu kľúčov medzi komunikujúcimi stranami cez nezabezpečený kanál. Výsledkom je vytvorenie symetrického šifrovacieho kľúča, ktorý slúži na šifrovanie komunikácie. Kľúč je tvorený všetkými účastníkmi, a nikdy nie je v otvorenej forme čo zabezpečuje ochranu pred prečítaním kľúča. Nevýhoda je bezbrannosť proti útoku Man in the middle, keďže tento protokol neumožňuje autentizáciu. [9]

1.3 Internet Protocol Security VPN

IPSec alebo aj Internet Protocol Security. Jedná sa o skupinu protokolov, ktoré poskytujú zabezpečenú IP komunikáciu medzi dvomi vzdialenými koncovými zariadeniami. Poskytuje utajenie údajov, integritu dát, autentifikáciu odosielateľa a Anti-replay ochranu. IPSec používa nasledujúce protokoly: [1] [3]

- Internet Key Exchange (IKE)
- Authentication Header (AH)
- Encapsulation Security Payload (ESP)

IPSec protokoly AH a ESP sa používajú buď na ochranu celého paketu alebo len jeho payloadu (dátová časť paketu bez hlavičky a zapätia). Podľa toho rozlišujeme dva IPSec módy:

Transportný mód: šifruje sa iba dátová časť, IP hlavička sa ponechá a doplní sa IPSec hlavičkou. Je používaný na ochranu protokolov vyšších vrstiev. Nie je kompatibilný s NAT-om. [1] [3]

Tunelový mód: šifruje sa celý paket (vrátane hlavičky) a doplní sa nová hlavička. Takže existujú dve IP hlavičky, vnútorná (pôvodná) a vonkajšia (nová). Tunelovací režim chráni prenos cez nedôveryhodnú sieť. [1] [3]

Pôvodný IP paket	IP hlavička	TCP hlavička	Dáta		
Transportný mód	IP hlavička	IPsec hlavička	TCP hlavička	Dáta	
Tunelový mód	IP hlavička	IPsec hlavička	IP hlavička	TCP hlavička	Dáta

Obrázok 1.1 Pôvodný IP paket, transportný a tunelovací mód

Security Association (SA)

Skupina algoritmov, ktorá zaisťuje združenie bezpečnostných služieb a identifikáciu chráneného sieťového prenosu medzi dvoma bodmi.

IPSec SA je definovaná vždy iba pre jeden smer, teda pre prichádzajúce alebo odchádzajúce pakety. Štandardne sú SA vytvárané párovo pre každý smer, a to buď dynamicky alebo manuálne. Dynamické SA majú definovanú životnosť na rozdiel od manuálnych, ktoré je potrebné ručne odstrániť. Identifikátor SPI (Security Parameter Index) ukázaním na položku v databáze pomáha určiť použité šifrovacie kľúče. Okrem SPI je na presné určenie šifrovacieho kľúča potrebné uviesť aj IP adresu príjemcu a použitý protokol AH alebo ESP. Táto trojica: SPI, IP adresa príjemcu, protokol (ESP alebo AH) je teda ukazovateľom do databázy (SAD) parametrov jednotlivých SA. [1] [8]

Authentication Header (AH)

Autentizačná hlavička (Obrázok 1.2) zabezpečuje integritu a autentizáciu zdroja dát. Obsah nie je šifrovaný a preto je možné ho prečítať, avšak nie je možné ho prepísať pretože je chránený integritou. Integrita paketov je v zaistená podpísaním pomocou algoritmu hash s kľúčom. Tak isto ako ESP poskytuje voliteľnú funkciu anti-replay [6].

Next header	Payload lenght	Reserved
SPI - security parameter index		
Sequence number		
HMAC- hash message authentication code		

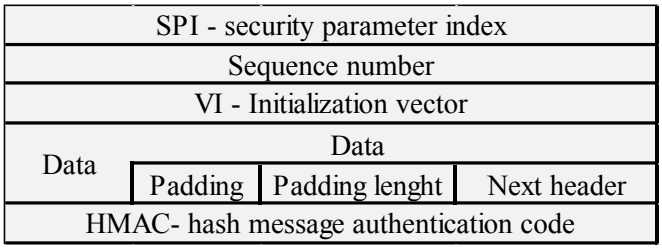
Obrázok 1.2 Hlavička AH [6]

Prvé pole hlavičky obsahuje 1 bajtovú položku Next header, ktorá ukazuje na ďalšiu hlavičku, ďalej veľkosť prenášaných dát s veľkosťou 1 bajt a posledné dva bity sú rezervované [6].

Ďalšie 32 bitové pole SPI slúži rovnako ako u ESP na označenie SA. Tretie pole je sekvenčné číslo, ktoré slúži ako anti-replay ochrana. Posledná štvrtá položka HMAC (hash message authentication code) je tvorená kódovým hashom o veľkosti 96 bitov [6].

Encapsulation Security Payload (ESP)

ESP zabezpečuje dôvernosť, integritu a tak isto autentickosť, ktorá je podobná ako u AH, ale v menšom rozsahu, keďže ESP overuje iba dáta. Výhodou je zabezpečenie proti odpočúvaniu pomocou šifrovania. Využívajú sa symetrické šifrovacie algoritmy ako napríklad DES, 3DES, AES a podobne[6].



Obrázok 1.3 Hlavička ESP[6]

Prvé pole v ESP hlavičke obsahuje položku SPI, ktorá označuje SA. Druhá položka nie je povinná a podobne ako u AH slúži ako anti-replay ochrana. Ďalšie, tretie pole je inicializačný vektor, ten sa využíva pri šifrovaní ako ochrana voči frekvenčnému útoku. IPSec používa blokové šifry a preto musí byť veľkosť hlavičky násobok 32 (IPv4) alebo 64 bitov (IPv6) a na to nám slúži štvrté pole padding, ktoré doplní potrebné bloky dát. Ďalšia časť padding lenght je určená na uloženie dĺžky doplnených blokov. Na koniec je pridaný HMAC algoritmus, ktorý zabezpečuje integritu dát. Algoritmus je aplikovaný na IP payload s vynechaním hlavičky. [6]

Ochrana pred útokom opakovaním (Anti-Replay) - poskytujú ju oba protokoly (AH, ESP), ide o ochranu pred útokom typu denial of service (DoS). DoS spočíva v tom, že útočník sa snaží opakovaným odosielaním starých paketov zahltiť príjemcu. IPSec pakety sú chránené pomocou sekvenčného čísla a posuvného okna. Po vytvorení SA je sekvenčné číslo inicializované na 0 a pred každým spracovaním paketu sa inkrementuje[6].

Internet Key Exchange (IKE)

IPSec využíva IKE protokol na vyjednávanie Security Association. IKE kombinuje atribúty prvej a druhej fázy za účelom zostavenia spojenia medzi účastníkmi. Všetky atribúty musia byť správne nakonfigurované, aby tunel nadviazal spojenie s druhým koncom. [3]

IKEv1 priebeh jednotlivých fáz:

Na vyjednávanie kľúčov a ďalších parametrov, ktoré zaisťujú bezpečné spojenie sa používa protokol ISAKMP. Pri protokole ISAKMP môžeme na výmenu kľúčov použiť ľubovoľný protokol. Protokol Internet Key Exchange (IKE) zabezpečuje spojenie od začiatku relácie, až po jej koniec a zaisťuje výmenu kľúčov. [3]

1. Fáza

V prvej fáze sa definuje IKE SA a dohadujú sa bezpečnostné parametre (šifrovací algoritmus, hash algoritmus, kľúče...), ktoré sú používané protokolom IKE. Ďalej dochádza k vzájomná autentizácií vzdialených koncov tunela pomocou autentizačnej metódy na ktorej sa dohodli. Táto fáza slúži na zabezpečenú výmenu informačných správ medzi koncovými uzlami. [3] [7]

V prvej fáze sú k dispozícií dva módy:

Hlavný mód: výmena správ medzi vzdialenými stranami prebehne tri krát a teda umožňuje bezpečnejšiu autentizáciu než agresívny mód. [9]

Agresívny mód: je menej náročný na výkon, pretože dochádza k výmene iba dvoch správ medzi vzdialenými stranami. [9]

2. Fáza

Výmena identít a certifikátov medzi vzdialenými stranami. Jednotlivé časti správ sú zašifrované vďaka kľúčom nastavených v prvej fáze. Možnosť využitia voliteľného zabezpečenia Perfect Forward Secrecy (PFS), kedy pri opätovnom vyjednávaní IKE SA alebo IPSec SA dochádza k tvorbe nových kľúčov, nezávislé na fáze 1. Vo fáze 2 sa používa iba quick mód. Cieľom je vytvorenie dvoch protismerných IPSec SA, ktoré slúžia na prenos dát.

Parametre, ktoré sa vyjednávajú IPSec SA: [9]

- Mód činnosti: transportný, tunelovací
- Spôsob zapuzdrenia: ESP alebo AH
- Druh symetrického šifrovania: DES, 3DES, AES...
- MTU (Maximum Unit Transfer) v rámci tunelu
- SPI
- Prenos, ktorý sa má zabezpečiť
- Doba trvania IPSec SA

IKEv2

Cisco ASA podporuje dve verzie IKEv1 a IKEv2. IKEv2 je podporovaný od verzie ASA 8.4.

- odolnejší voči sieťovým útokom, dokáže napríklad zmierniť DoS útok kontrolovaním IP adresy iniciátora [10]
- zlepšuje spoluprácu IPSec medzi rôznymi výrobcami zariadení pomocou technológií ako Dead Peer Detection, NAT Traversal alebo Iniciátor spojenia
- používa asymetrickú autentizáciu

IKEv2 je novšou verziou IKEv1. Je definovaná v RFC 7296, RFC 7427 a vlastnosťami je veľmi podobná IKEv1. Nie je spätne kompatibilná s verziou IKEv1. Ak jedna strana tunela padne, posiela informáciu vzdialenému peerovi. [10]

IKEv2 má rovnako ako IKEv1 dve fázy vyjednávania. Prvá fáza sa nazýva IKE_SA_INIT a druhá IKE_AUTH. Na konci druhej fázy je vytvorený prvý CHILD_SA, ktorý je v IKEv1 definovaný ako IPSec SA. V druhej verzií sú k dispozícií nové Diffie-Hellman hodnoty a takisto kombinácie šifrovania a hashovania a naopak už nie je sú k dispozícií hlavný a agresívny mód. IKEv2 počúva na UDP porte 500 a 4500 (IPSec NAT traversal). [1] [10]

Postup pri zostavovaní spojenia

Na začiatku prebehne výmena správ, kedy sa medzi komunikujúcimi stranami vytvorí zabezpečený kanál a každá ďalšia komunikácia je šifrovaná. Prvá správa IKE_SA_INIT je poslaná iniciátorom vzdialenému zariadeniu a obsahuje návrh na zabezpečenie, šifrovacie a hashovacie algoritmy, Diffie-Hellman kľúče a Nonces. Rovnaké parametre obsahuje aj druhá správa odoslaná zo vzdialeného zariadenia k iniciátorovi. [1] [10]

Tretia a štvrtá správa IKE_AUTH je už šifrovaná a autentifikovaná pomocou IKE SA, ktoré bolo vytvorené v prvej výmene IKE_SA_INIT. Tieto správy slúžia k overeniu, potvrdeniu identít iniciátora a vzdialeného zariadenia, k výmene certifikátov (ak sú k dispozícií), k overeniu predchádzajúcich správ a vytvoreniu prvého CHILD_SA. [1] [10]

PRF (Pseudo-random function) je použitý ako algoritmus na odvodenie kľúča a hash operácií, ktoré sú vyžadované pre IKEv2 a používa sa vo fáze vyjednávania. V IKEv1 je hodnota integrity a PRF rovnaká, ale v IKEv2 môžeme definovať inú hodnotu pre integritu a inú pre PRF. [1] [2]

RRI (reverse route injection) je schopnosť automaticky vložiť do smerovacieho procesu statickú cestu, pre tie siete alebo klientov, ktorí sú chránení vzdialeným koncom tunela. Dynamické vloženie cesty funguje iba vtedy, ak je klient pripojený, ak sa odpojí, odstráni sa cesta zo smerovacej tabuľky. Nevýhodou RRI je, že pre každého klienta je v smerovacej tabuľke samostatný záznam s maskou 32 bitov, ak by sme mali pripojených viac klientov, smerovacia tabuľka by bola neprakticky dlhá. [1]

1.4 Secure Sockets Layer VPN

SSL VPN poskytuje vzdialený prístup takmer z hoci akého miesta pripojeného k Internetu a to iba použitím webového prehliadača, ktorý štandardne podporuje SSL šifrovanie. Tým umožníme ľubovoľnému autentizovanému užívateľovi zabezpečený prístup do vzdialenej siete. Secure Sockets Layer (SSL) pracuje na prezentačnej vrstve, nad protokolom TCP. Možnosti použitia SSL VPN nájdeme na obrázku 1.5.

TLS/DTLS

Pre vytvorenie zabezpečeného spojenia medzi klientom a serverom sa používa protokol TLS. TLS poskytuje spojovo-orientovanú komunikáciu a je akoby spojkou medzi aplikačnou a transportnou vrstvou pri TCP spojení. [11]

Aby sa klienti vyhli oneskoreniu, napríklad pri sledovaní videa využívajú DTLS protokol (Datagram Transport Layer Security), ktorý je modifikovanou verziou TLS s rovnakým zabezpečením. DTLS pracuje s protokolom UDP čím je výhodný pre časovo citlivé aplikácie, ktoré vyžadujú VPN spojenie. Na druhej strane ide o nespojovo orientovaný protokol s bezpečnostnými prvkami.

Postup pri zostavovaní spojenia a výmena TLS/SSL správ

V prvom kroku dochádza k vyjednávaniu šifrovacích informácií medzi klientom a serverom. Ide o metódu výmeny kľúča a metódu šifrovania. Ďalej je možné zabezpečiť overenie identity servera

voči klientovi, nevyhnutnosť závisí na použitej aplikácií. Posledným krokom je výmena kľúčov pomocou asymetrického šifrovania, ktoré budú použité na šifrovane dát. [11]

Proces autentifikácie a zostavenia šifrovaného kanála (Obrázok 1.4) pozostáva z týchto krokov:

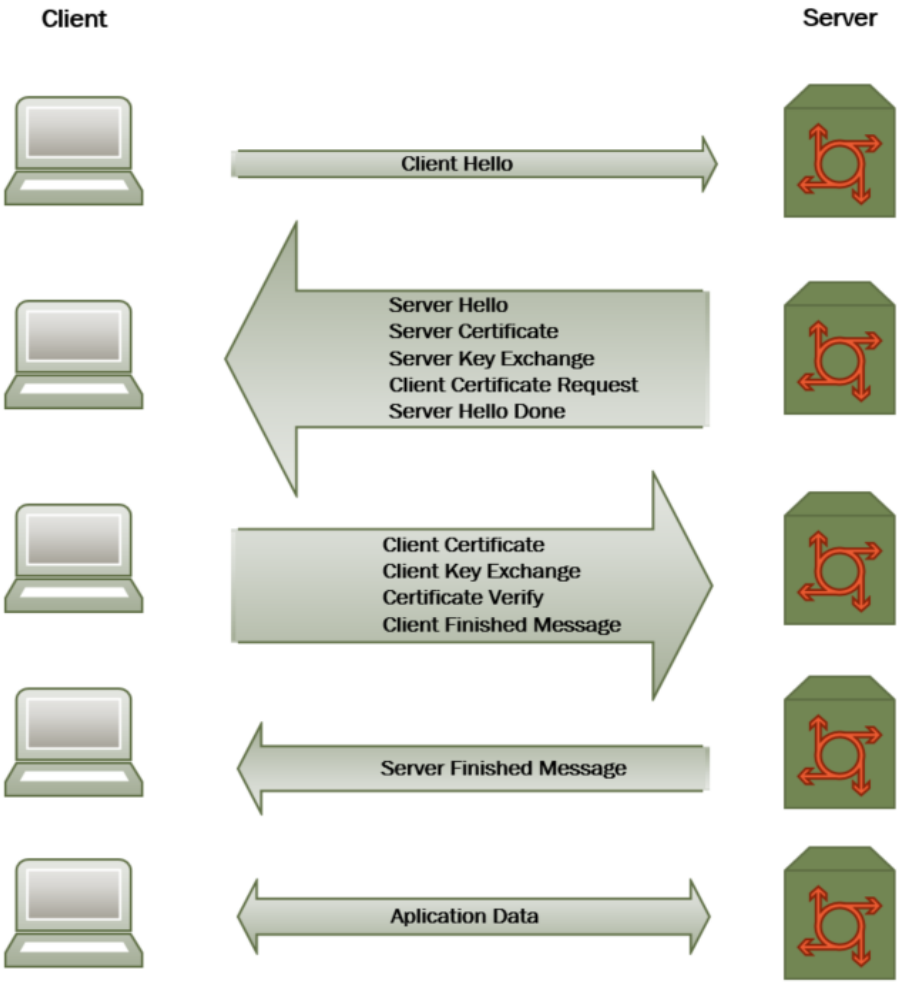
- **Klient iniciuje spojenie**

Prvá správa, ktorú posiela klient a iniciuje spojenie je *Client Hello* správa serveru a obsahuje číslo verzie, náhodné číslo klienta, ktoré slúži na odvodenie kľúča, parametre zabezpečenia ako napríklad TLS_RSA_WITH_DES_CBC_SHA.

- **Server → klient**

Server odpovedá správou *Server Hello*, ktorá obsahuje rovnaké parametre ako v predchádzajúcej správe a ak sa na týchto parametroch obe strany dohodnú vymieňajú sa ďalšie správy.

Ďalej je zo strany servera posielaná správa *Server Certificate,* ktorá obsahuje verejný kľúč servera. Taktiež môže obsahovať certifikát podpísaný certifikačnou autoritou, v ktorom si klient overuje meno servera v certifikáte, ak meno servera nesedí webový prehliadač informuje klienta o neplatnom certifikáte.



Obrázok 1.4 Výmena správ medzi klientom a serverom pri zostavovaní TLS/SSL spojenia

Správa *Server Key Exchange* je posielaná v prípade, že certifikát serveru neobsahuje verejný kľúč. Tento kľúč je nahradený dočasným kľúčom a slúži na zašifrovanie správy *Client Key* Exchange.

Ďalšia správa *Client Certificate Request* je voliteľná a posielaná v prípade, že server vyžaduje autentifikáciu klienta pomocou certifikátu.

Server *Hello Done* správa indikuje, že server ukončil svoju sekvenciu správ a čaká na odpoveď od klienta.

- **Klient → server**

Správa *Client Certificate* je odpoveďou klienta v prípade, že si server certifikát vyžiadal, certifikát potom obsahuje verejný kľúč klienta.

Client Key Exchange správa obsahuje pre-master tajný kľuč zašifrovaný pomocou verejného kľúča z certifikátu servera. Ak ho server dešifruje, klient si je istý, že server má správny privátny kľúč.

Certificate Verify správa je posielaná len v prípade, že klient poslal správu *Client Certificate* a obsahuje dlhý podpis na overenie pravosti certifikátu od klienta.

Client Finished je hash všetkých predchádzajúcich správ a slúži na zabezpečenie autenticity medzi komunikujúcimi stranami.

- **Server → klient**

Server Finished ak je klient schopný dešifrovať správu a overiť hash, je si istý, že TLS/SSL handshake bol úspešný a kľúče na oboch stranách sú zhodné.

- **Klient ⇔ server**

Application Data definuje samotný zabezpečený prenos dát pomocou dohodnutých parametrov.

SSL VPN módy

Cisco ASA podporuje všetky tri módy SSL VPN, ktoré sú:

Clientless

Vzdialenému klientovi postačuje iba webový prehliadač s podporou SSL protokolu aby mohol pristupovať, napríklad do svojej privátnej siete. SSL klient sa v tomto móde môže pripájať do svojej internej siete pomocou protokolu HTTPS alebo zdieľať, vytvárať a meniť súbory v internej sieti pomocou SSL tunela. [1] [5]

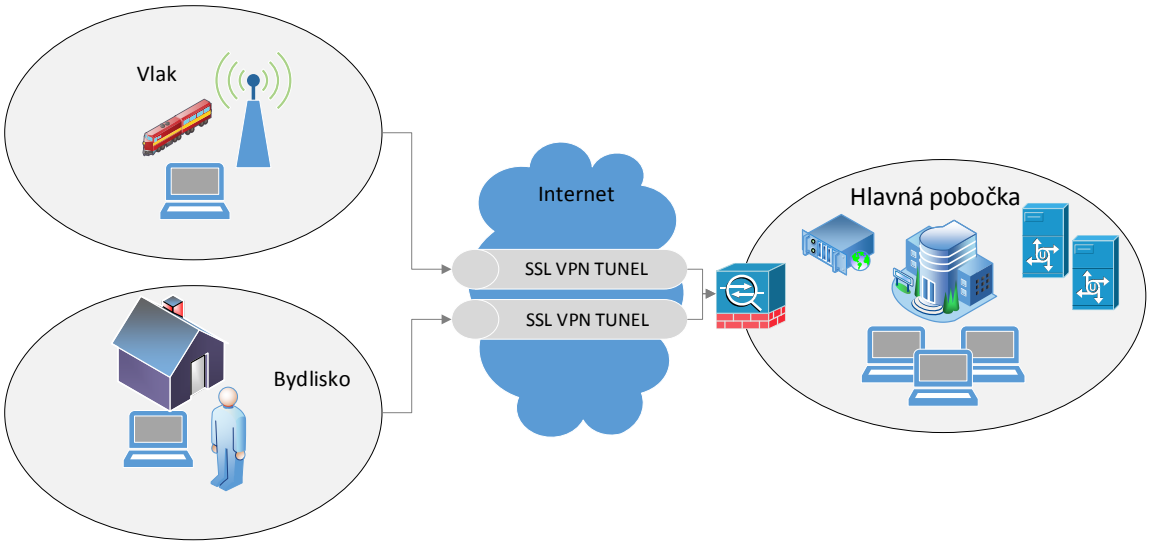
Thin client

Mód, pri ktorom dochádza k presmerovaniu portu. Vzdialený klient musí mať nainštalovaný Java applet na vytvorenie zabezpečeného spojenia pomocou protokolu TCP. Tento mód rozširuje šifrovacie schopnosti webového prehliadača. Umožňuje vzdialený prístup k aplikáciám pracujúcich na TCP, ako napríklad protokoly na odosielanie a prijímanie pošty alebo SSH. [1] [5]

SSL VPN client (Full tunnel)

Aby mal vzdialený klient plný prístup k privátnej sieti cez SSL tunel musí mať nainštalovaného SSL VPN klienta. Vzdialené zariadenia v tunelovacom móde posielajú celý unicastový tok pomocou

TCP, UDP alebo ICMP protokolu. SSL klienti sa môžu pripájať do internej siete na HTTPS, DNS, SSH alebo Telnet servery. Full tunnel mód je najviac preferovaný, pretože po úspešnej autentifikácií používateľa je automaticky vytvorený VPN tunel. Po ukončení spojenia môže byť Cisco AnyConnect VPN klient odstránený alebo ponechaný na stanici.[1] [5]



Obrázok 1.5 Využitie SSL VPN

1.5 Layer 2 Tunneling Protocol

Ide o tunelovací protokol a slúži na vytvorenie zabezpečenej komunikácie v privátnych sieťach medzi vzdialeným zariadením a firemnou sieťou. [12]

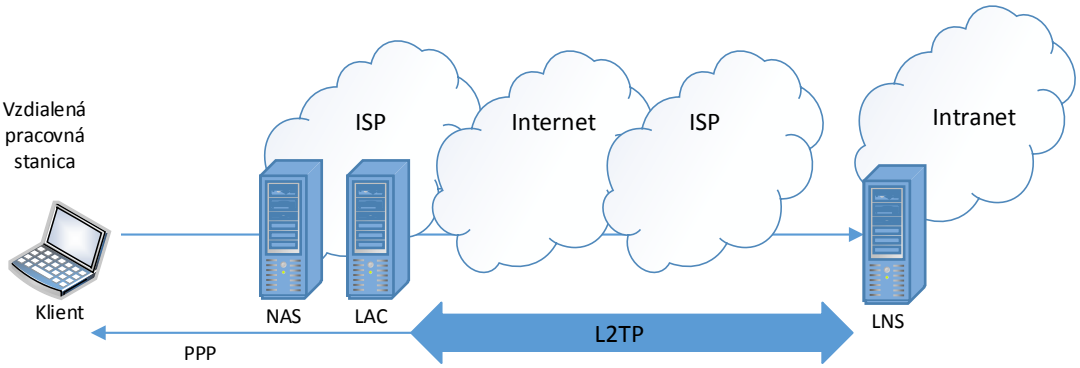
- Umožňuje vytvárať spojenie na druhej vrstve
- Zabezpečuje vzdialený prístup do internej siete
- Vznikol zlúčením protokolov: Point-to-Point Tunneling Protocol (PPTP) a Layer 2 Forwarding (L2F)
- Nezabezpečuje šifrovanie ani dôvernosť dát

Architektúra L2TP (Obrázok 1.6) je zložená s týchto komponentov: [12]

Prístupový koncentrátor LAC (L2TP Access Concetrator) nachádza sa na prístupovom mieste do siete ISP (POP ISP) a zaisťuje fyzické spojenie vzdialeného používateľa. Z koncentrátora LAC vedie spojenie L2TP na jeden alebo viacero LNS serverov, na ktorých tunely L2TP končia.

Sieťový server LNS (L2TP Network Server) ukončuje spojenia L2TP. Na ukončenie týchto L2TP spojení používateľov na LNS sa používa iba jedno spojenie.

Sieťový prístupový server NAS (Network Access Server) je point-to-point prístupové zariadenie, ktoré zaisťuje prístup cez linky PSTN zariadenia pre vzdialených používateľov alebo ISDN.



Obrázok 1.6 Popis zariadení, organizácií a služieb pri vytváraní L2TP tunela

Priebeh vytvárania L2TP tunela [12]

- Vzdialený klient zahájí pripojenie prostredníctvom protokolu PPP na server NAS
- Server NAS príjme žiadosť o pripojenie
- Pomocou autentizačného servera (napr. RADIUS) sa vykoná overenie koncového klienta, ktorá prebieha na serveri NAS
- LAC iniciuje vytvorenie L2TP spojenia na základe požiadavky od klienta. Každý pokus o pripojenie otvára spojenie riadene koncentrátorom
- Vzdialený klient je overovaný autentizačným serverom na bráne LNS, pred povolením na vytvorenie tunela
- Server LNS akceptuje pripojenie a vytvorí sa tunel L2TP
- Server NAS zaprotokoluje akceptovanie
- Server LNS si so vzdialeným klientom vyjednáva PPP podmienky
- Vytvorí sa tunel, ktorým sú prenášané údaje medzi vzdialeným klientom a LNS serverom

Protokol L2TP podporuje dva typy tunelov a to povinný a dobrovoľný tunel

Povinný tunel

L2TP je zriadený od LAC cez ISP až k LNS. Tento typ tunela je používaný s podporou poskytovateľa, ktorý musí podporovať L2TP a na základe autentizačných informácií určiť, či je možné použiť konkrétnu reláciu. Povinný tunel nevyžaduje zmeny na strane vzdialeného klienta. Neumožňuje klientovi prístup na Internet. [12]

Dobrovoľný tunel

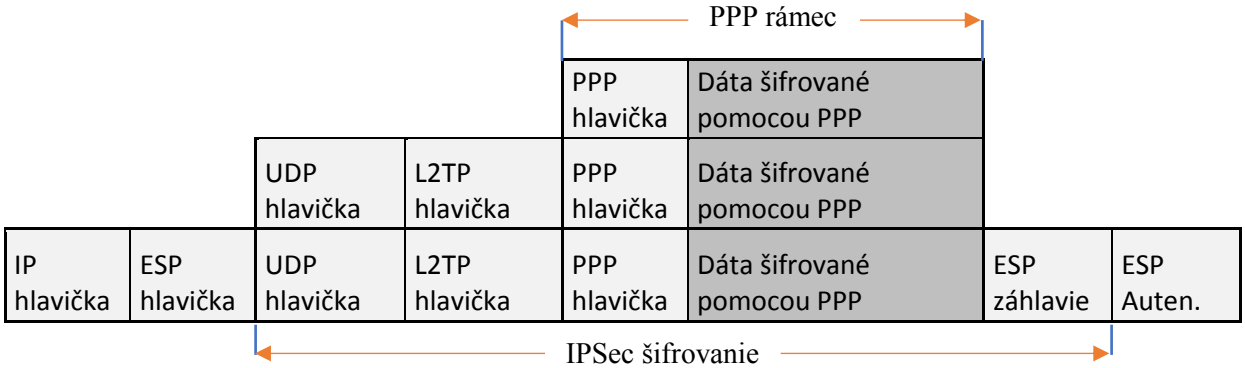
Je podobný PPTP a pre ISP transparentný. Vyžaduje podporu L2TP na strane klienta a umožňuje klientovi prístup na Internet. [12]

L2TP over IPSec

Pakety, ktoré sú prenášané L2TP tunelom nie sú zabezpečené pred útočníkom. Tunel L2TP rámec vytvoríme zabalením L2TP rámca najprv do UDP datagramu s portom 1701 a potom do IP paketu. Adresy v IP pakete označujú začiatok a koniec tunela. Na vytvorenie zabezpečenej komunikácie medzi dvoma komunikujúcimi stranami sa používa bezpečnostná verzia IPSec. Pri zabezpečení používame spolu s IPSec protokoly AH, ESP a IKE. Postupné zabalenie PPP rámca môžeme vidieť na Obrázku 1.7.

Priebeh vytvorenia L2TP/IPSec tunela [1]

1. Klient spustí L2TP klienta, ktorý je nastavený tak aby podporoval IPSec
2. Klientske zariadenie iniciuje spojenie a vyjednávajú sa parametre na vytvorenie bezpečného kanála, ktorý bude slúžiť na výmenu kľúčov
3. Po úspešnom vytvorení prvej fázy sú zostavené dva bezpečné kanále pre šifrovanie a autentifikáciu dát (2. fáza). Šifrovaný L2TP prenos je prenášaný dátovým kanálom a smerovaný na UDP port 1701 (pri použití IPSec na port UDP 500)
4. Po zostavení IPSec spojenia, klient iniciuje L2TP spojenie s podporou IPSec
5. Autentifikácia pomocou vopred nastavených autentifikačných parametrov je použitá na overenie L2TP spojenia. Všetky PPP alebo L2TP atribúty sú vyjednávane až po úspešnej autentifikácií klienta
6. Po zostavení L2TP spojenia používateľ posiela dáta zabalené v L2TP pakete šifrovanom pomocou IPSec a posielaný druhému koncu cez nezabezpečenú sieť



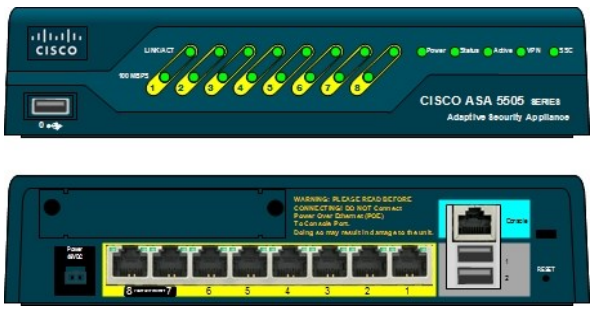
Obrázok 1.7 Postupné zabalenie PPP rámca pri prenose zabezpečeným L2TP/IPSec tunelom

2 Návrh a realizácia VPN s využitím firewalu ASA 5505

Táto kapitola je zameraná na prakitckú časť diplomovej práce, v ktorej sú navrhnuté jednotlivé zapojenia a tie sú následne konfigurované na zariadení Cisco ASA 5505.

2.1 Cisco ASA 5505

Cisco ASA je názov pre sieťové zariadenie firewall vytvorené spoločnosťou Cisco. Séria ASA 5500 bola uvedená v roku 2005 a nahradila líniu Cisco PIX. Cisco ASA používa operačný systém Linux namiesto Finesse/Pix OS, ktorý bol používaný v starších Cisco PIX zariadeniach. Je kombináciou firewallu, základnej funkcie brány, anti-X (ochrana proti spyware, phising a podobne), spája funkcie IPS a VPN koncentrátora. Ide teda o zariadenie, ktoré poskytuje ochranu počítačovej siete. Cisco ASA začína malými modelmi 5505, 5510, ktoré nachádzajú svoje využitie v menších firmách a pokračuje až k najvýkonnejším 5580, 5585. Ide teda o zariadenie, ktoré poskytuje ochranu počítačovej sieti rôzneho rozsahu. [1] [4]



Obrázok 2.1 Cisco ASA 5505 [13]

Toto zariadenie môžeme konfigurovať dvoma spôsobmi a to pomocou ASDM (Adaptive Security Device Manager), čo je Java aplikácia, ktorú je možne spustiť cez webové rozhranie alebo štandardne cez príkazový riadok. [4]

My budeme mať k dispozícii najnižšiu radu ASA 5505 (Obrázok 2.1), ktorá má svoje využite v malých sieťach. ASA 5505 podporuje VPN, ktoré môžu slúžiť pre vzdialený prístup do firemnej siete alebo na prepojenie pobočiek pomocou Site-to-Site VPN.

VPN podporované zariadením Cisco ASA 5505:

IPSec VPN

- Site-to-Site
- Remote Access

SSL VPN

- Thin client
- Clientless SSL VPN
- Cisco SSL VPN Client (AnyConnect VPN)

L2TP/IPSec VPN a PPTP VPN

Úvod do praktickej časti

V praktickej časti sme konfigurovali 3 typy tunelov, s toho bol jeden typu LAN to LAN (L2L) a druhé dva typu remote access. Pri L2L tunely sme pracovali s technológiou IPSec a pri type remote access sme využili SSL VPN a L2TP/IPSEC VPN. Celá realizácia praktickej časti prebiehala na VŠB-TUO v učebni EB215.

Pred začatím konfigurácie je vhodné povoliť protokol ICMP a to z dôvodu testovania konektivity. ICMP protokol povolíme nasledovne:

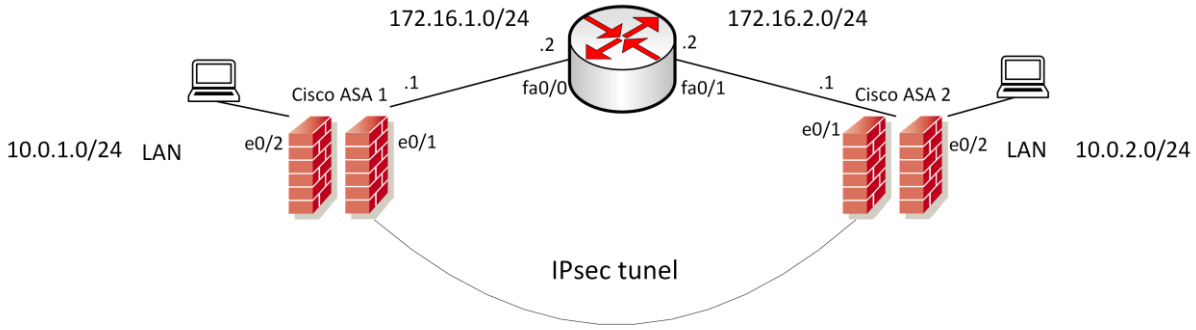
policy-map global_policy

class inspection_default

inspect icmp

2.2 Technológia IPSec VPN (IKEv2)

Pri návrhu IPSec VPN sme využili dve zariadenia ASA 5505, medzi ktorými sme vytvorili IPSec tunel. Do stredu medzi ASA zariadenia sme vložili router, na ktorom sme nakonfigurovali rozhrania a priradili IP adresy. Ku každému zariadeniu ASA sme na rozhranie INSIDE pripojili PC. Z dôvodu odchytenia komunikácie sme do siete 172.16.1.0/24 pripojili HUB a do neho sme pripojili PC.



Obrázok 2.2 Schéma zapojenia IPSec tunela

2.2.1 Konfigurácia IPSec VPN na zariadení ASA 5505

Najskôr je potrebné nakonfigurovať rozhrania. Konfigurácia rozhraní na zariadení ASA 5505 je odlišná v tom, že IP adresy nie sú pridelené na fyzické rozhranie, ako to býva u Cisco smerovačoch alebo na vyšších radách ASA, ale na virtuálne LAN rozhranie. Na fyzických rozhraniach iba vytvoríme prístupovú VLAN a zapneme rozhranie.

interf eth 0/1

switch acc vlan 2

no shutdown

Na VLAN je okrem IP adresy potrebné definovať nameif. Defaultne sú dva typy názvov, ku ktorým je automaticky priradený level zabezpečenia. Inside má najvyššiu hodnotu zabezpečenia 100 a slúži pre vnútorné siete, LAN siete s najvyššou úrovňou zabezpečenia a potom je názov *OUTSIDE*, ktorý má najnižšiu úroveň zabezpečenia s hodnotou 0, tento port je priamo pripojený do Internetu.

```
interface vlan 2
 nameif OUTSIDE
 security-level 0
 ip address 172.16.1.1 255.255.255.0
 no shutdown

interface vlan 3
 nameif INSIDE
 security-level 100
 ip address 10.0.1.1 255.255.255.0
 no shutdown
```

V prvej časti konfigurujeme IKEv2 politiku, ktorej ekvivalentom v IKEv1 je ISAKMP politika. Na vytvorenie ISAKMP SA je nevyhnutné definovať šifrovanie a hashovanie, výmenu kľúčov, ktorá prebieha pomocou Diffie-Helman algoritmu. V našom prípade sme zvolili hodnotu 14, ktorá definuje 2048 bitovú skupinu DH a je odporúčaná firmou Cisco do roku 2030. Aspoň jeden parameter pre šifrovanie a hashovanie musí byť zhodný na obidvoch stranách, aby došlo k vytvoreniu tunela. Vo verzii IKEv1 bol parameter lifetime povinný vo verzii IKEv2 je tento parameter voliteľný.

```
crypto ikev2 policy 1
encryption aes-192
integrity sha512 sha256
group 19 14 5
prf sha256 sha
crypto ikev2 enable OUTSIDE
```

Ďalej je potrebné konfigurovať IKEv2 proposal, kde nastavíme metódy zabezpečenia prevádzky šifrovanie, hashovanie a v IKEv2 už iba s využitím protokolu ESP. Konfigurácie *IPSec-proposal* je ekvivalentom *transform-set* v IKEv1

```
crypto IPSec ikev2 IPSec-proposal VPNZAB
protocol esp encryption aes-192 aes
protocol esp integrity sha-1
```

Pomocou prístupového zoznamu určíme, ktorá prevádzka a v akom smere bude zabezpečená. V krypto mapách priradíme prístupový zoznam a metódy zabezpečenia prevádzky, nastavíme adresu vzdialeného konca tunela a určime rozhranie, cez ktoré bude daná prevádzka prechádzať. Posledným príkazom je *crypto map TrafficSP 1 set reverse-route*, ktorým nastavíme vloženie statickej cesty do vzdialenej lokálnej siete.

access-list 101 permit ip 10.0.1.0 255.255.255.0 10.0.2.0 255.255.255.0

crypto map TrafficSP 1 match address 101

crypto map TrafficSP 1 set peer 172.16.2.1

crypto map TrafficSP 1 set ikev2 IPSec-proposal VPNZAB

crypto map TrafficSP interface OUTSIDE

crypto map TrafficSP 1 set reverse-route

V poslednom kroku určíme typ tunela a nastavíme pred-zdieľané kľúče, v IKEv2 je novinkou lokálny a vzdialený pred-zdieľaný kľúč, ktorými tak isto zvýšime zabezpečenie komunikácie. Smerovanie môžeme riešiť jednoducho, pomocou statickej cesty. Pri nastavovaní *tunnel-group* je trochu mätúce vyžadované vloženie názvu, ten slúži iba v prípade, že ide o autentizáciu pomocou certifikátu, v opačnom prípade je potrebné vložiť IP adresu peera.

tunnel-group 172.16.2.1 type IPSec-l2l

tunnel-group 172.16.2.1 IPSec-attributes

ikev2 remote-authentication pre-shared-key S$vS3e9TD-Q

ikev2 local-authentication pre-shared-key kI4rq5asE-W

exit

route outside 0.0.0.0 0.0.0.0 172.16.1.2

2.2.2 Overenie konfigurácie IPSec VPN

Vo vrchnej časti obrázka 2.3 môžeme vidieť vyjednané parametre, ktoré slúžia na bezpečnú výmenu riadiacich informácií, ďalej sú tam informácie o lokálnom a vzdialenom konci tunela, teda IP adresy, SPI, rola a podobne. V spodnej časti obrázku 2.3 sa nachádza Child SA parametre, ktoré definujú zabezpečenie dátovej komunikácie medzi koncovými sieťami.

```
ASA1(config)# sh crypto ikev2 sa det

IKEv2 SAs:

Session-id:10, Status:UP-ACTIVE, IKE count:1, CHILD count:1

Tunnel-id                Local                Remote      Status          Role
989539981        172.16.1.1/500        172.16.2.1/500      READY     INITIATOR
      Encr: AES-CBC, keysize: 192, Hash: SHA512, DH Grp:14, Auth sign: PSK, Auth verify: PSK
      Life/Active Time: 86400/393 sec
      Session-id: 10
      Status Description: Negotiation done
      Local spi: 2B37AB8834835356       Remote spi: C45C3ACFFBCBD06F
      Local id: 172.16.1.1
      Remote id: 172.16.2.1
      Local req mess id: 19             Remote req mess id: 17
      Local next mess id: 19            Remote next mess id: 17
      Local req queued: 19              Remote req queued: 17
      Local window: 1                   Remote window: 1
      DPD configured for 10 seconds, retry 2
      NAT-T is not detected
Child sa: local selector  10.0.1.0/0 - 10.0.1.255/65535
          remote selector 10.0.2.0/0 - 10.0.2.255/65535
          ESP spi in/out: 0x1add1d84/0x169a50e3
          AH spi in/out: 0x0/0x0
          CPI in/out: 0x0/0x0
          Encr: AES-CBC, keysize: 192, esp_hmac: SHA96
          ah hmac: None, comp: IPCOMP NONE, mode tunnel
```

Obrázok 2.3 IKEV2 SA

Na obrázku 2.4 môžeme vidieť statickú cestu vloženú pomocou funkcie RRI, ide o vzdialenú lokálnu sieť na druhej strane tunela.

```
ASA1(config)# sh route

Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is 172.16.1.2 to network 0.0.0.0

C    172.16.1.0 255.255.255.0 is directly connected, OUTSIDE
S    10.0.2.0 255.255.255.0 [1/0] via 172.16.1.2, OUTSIDE
S*   0.0.0.0 0.0.0.0 [1/0] via 172.16.1.2, OUTSIDE
ASA1(config)#
ASA2(config)# sh route

Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is 172.16.2.2 to network 0.0.0.0

C    172.16.2.0 255.255.255.0 is directly connected, OUTSIDE
S*   0.0.0.0 0.0.0.0 [1/0] via 172.16.2.2, OUTSIDE
```

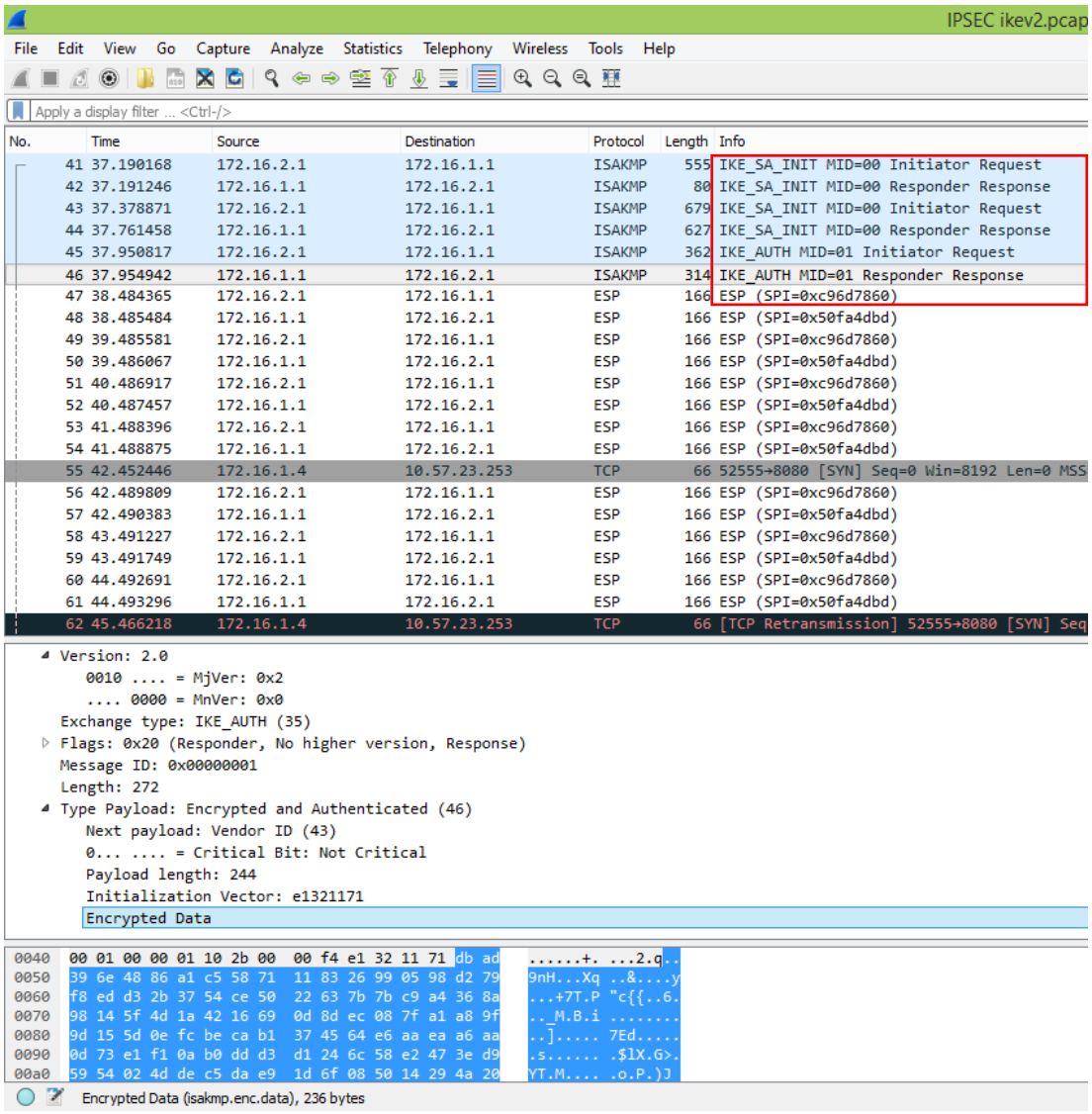
Obrázok 2.4 Výpis smerovacích informácií

Na obrázku 2.5 môžeme vidieť podrobné informácie týkajúce sa parametrov IPSec, sú to informácie o dátovom toku, podrobný výpis nastavení IPSec SA, identifikácia vzdialenej a lokálnej siete a IP adresa vzdialeného konca tunela.

```
ASA2(config)# sh ipsec sa
interface: OUTSIDE
    Crypto map tag: TrafficSP, seq num: 1, local addr: 172.16.2.1

      access-list 101 extended permit ip 10.0.2.0 255.255.255.0 10.0.1.0 255.255.255.0
      local ident (addr/mask/prot/port): (10.0.2.0/255.255.255.0/0/0)
      remote ident (addr/mask/prot/port): (10.0.1.0/255.255.255.0/0/0)
      current_peer: 172.16.1.1


      #pkts encaps: 4, #pkts encrypt: 4, #pkts digest: 4
      #pkts decaps: 4, #pkts decrypt: 4, #pkts verify: 4
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 4, #pkts comp failed: 0, #pkts decomp failed: 0
      #pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0
      #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
      #TFC rcvd: 0, #TFC sent: 0
      #Valid ICMP Errors rcvd: 0, #Invalid ICMP Errors rcvd: 0
      #send errors: 0, #recv errors: 0

      local crypto endpt.: 172.16.2.1/500, remote crypto endpt.: 172.16.1.1/500
      path mtu 1500, ipsec overhead 74(44), media mtu 1500
      PMTU time remaining (sec): 0, DF policy: copy-df
      ICMP error validation: disabled, TFC packets: disabled
      current outbound spi: 9A51733E
      current inbound spi : 6A4ED465

    inbound esp sas:
      spi: 0x6A4ED465 (1783551077)
         transform: esp-aes-192 esp-sha-hmac no compression
         in use settings ={L2L, Tunnel, IKEv2, }
         slot: 0, conn_id: 16384, crypto-map: TrafficSP
         sa timing: remaining key lifetime (kB/sec): (4008959/28630)
         IV size: 16 bytes
         replay detection support: Y
         Anti replay bitmap:
          0x00000000 0x0000001F
    outbound esp sas:
      spi: 0x9A51733E (2589029182)
         transform: esp-aes-192 esp-sha-hmac no compression
         in use settings ={L2L, Tunnel, IKEv2, }
         slot: 0, conn_id: 16384, crypto-map: TrafficSP
         sa timing: remaining key lifetime (kB/sec): (4331519/28630)
         IV size: 16 bytes
         replay detection support: Y
         Anti replay bitmap:
          0x00000000 0x00000001
```

Obrázok 2.5 Podrobné informácie o nastavení Security Association (SAs)

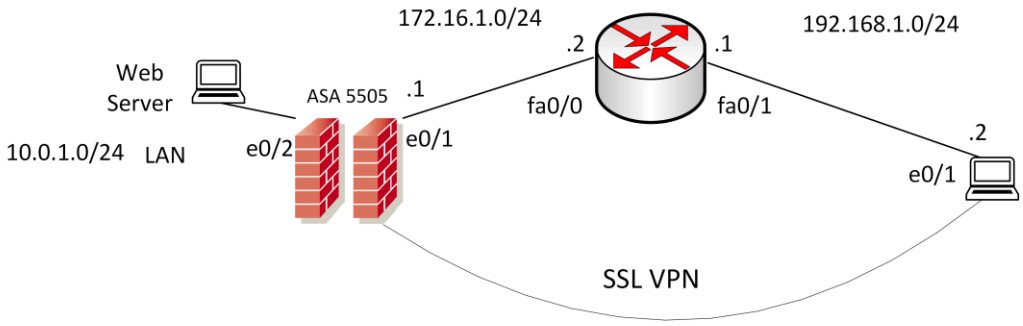
Na obrázku 2.6 môžeme vidieť výmenu IKEv2 správ až po zostavenie zabezpečeného IPSec spojenia v tunelovacom móde.



Obrázok 2.6 Zachytenie IKEv2 komunikácie pomocou programu Wireshark

2.3 Technológia SSL VPN

Prvá Remote access VPN, ktorú sme konfigurovali, bola SSL VPN typu full tunnel, kde po overení prihlasovacích údajov a certifikátu môže vzdialene, napríklad telekomuter pristupovať do internej siete. Pre overenie sme vytvorili web server, na ktorý sme mali po prihlásení sa do VPN siete prístup.



Obrázok 2.4 Schéma zapojenia SSL VPN

2.3.1 Konfigurácia SSL VPN na zariadení ASA 5505

Konfiguráciu rozhraní sme už popísali v podkapitole IPSec VPN, je rovnaká aj pre SSL VPN a teda sa ňou nebudeme ďalej zaoberať. Pred konfiguráciou autentifikačného servera je vhodné použiť príkaz *crypto key zeroize rsa*, ktorý odstráni všetky vygenerované RSA kľúče. Ak by sa nám server nepodarilo nastaviť, pretože sa už nachádza v konfigurácií, môžeme použiť príkaz *no crypto ca server*, ktorý vymaže tento server vymaže.

Cisco ASA konfigurujeme ako autentifikačný server, ktorý vygeneruje certifikát a aj pomocou neho sa musia používatelia autentifikovať. Popri vytváraní servera sa taktiež vygeneruje pár RSA kľúčov, takže nie je potrebné ich osobitne generovať.

Lokálnemu serveru môžeme priradiť rôzne parametre, ako napríklad vydavateľa certifikátu, obnovenie OTP, dĺžku kľúča, platnosť certifikátu, a podobne.

crypto ca server

issuer-name CN=vsb.cz

subject-name-default CN=vsb.cz

otp expiration 168

keysize 2048

lifetime certificate 120

lifetime ca-certificate 265

no shutdown

V ďalšom kroku pridáme užívateľa, povolíme jeho priradenie k certifikátu a definujeme informácie o užívateľovi. Navyše je možné uviesť emailovú adresu, na ktorú bude doručené OTP heslo alebo ho zobrazíme v konfigurácií, ako v našom prípade.

crypto ca server user-db add marko dn CN=marko,OU=TAC

crypto ca server user-db allow marko display-otp

Konfigurácia lokálneho rozsahu, z ktorého budú priradzované IP adresy jednotlivým anyconnect klientom.

ip local pool VPN_Pool 10.0.1.3-10.0.1.200 mask 255.255.255.0

Ďalej máme konfiguráciu, vďaka ktorej sa nám pomocou prehliadača zobrazí prihlasovacie okno a tiež mapovanie cesty k inštalačnému súboru *anyconnect-win-4.3.02039-k9.pkg*.

w*ebvpn*

enable outside

anyconnect image disk0:/ anyconnect-win-4.3.02039-k9.pkg

anyconnect enable

tunnel-group-list enable

Definovanie prihlasovacích údajov a group-policy, ktorú môžeme konfigurovať ako internú, alebo externú. Interná sa nachádza na zariadení ASA, na ktorom vytvárame konfiguráciu. *V group-policy*, sme nastavili rôzne parametre tunela a to napríklad typ tunela, počet súčasne prihlásených VPN klientov, čas za ktorý sa tunel stáva nečinným, ak ním neprechádza žiadna komunikácia a podobne.

username marko password cKe9asdp8

group-policy SSL_VPN_GR internal

group-policy SSL_VPN_GR attributes

vpn-tunnel-protocol ssl-client

vpn-simultaneous-logins 30

vpn-idle-timeout 120

dns-server none

wins-server none

default-domain none

V konfigurácií *tunnel-group* definujeme, akým spôsobom sa klient overí voči autentizačnému serveru, v našom prípade lokálne voči ASA. Ďalej priradíme východzu politiku a rozsah IP adries, ktoré budú prideľované VPN klientovi. Pomocou tunnel-group môžeme jednoducho pridávať VPN klientov bez toho aby sme nastavovali *group-policy*.

tunnel-group SSL_VPN_TNLGR type remote-access

tunnel-group SSL_VPN_TNLGR general-attributes

authentication-server-group LOCAL

default-group-policy SSL_VPN_GR

address-pool VPN_Pool

tunnel-group SSL_VPN_TNLGR webvpn-attributes

authentication aaa certificate

group-alias SSL_VPN_TNLGR enable

V poslednom kroku sme konfigurovali ASA ako certifikačnú autoritu ako trustpoint, ktorá vygeneruje a podpíše certifikát. Ten slúži na overenie identity zariadenia cisco ASA.

crypto ca trustpoint IdentityCert

enrollment self

subject-name CN=vsb.cz,CN=172.16.1.1

fqdn ciscoasa.vsb.cz

keypair LOCAL-KEYPAIR

exit

crypto ca enroll IdentityCert noconfirm

ssl trust-point IdentityCert outside

2.3.2 Overenie konfigurácie SSL VPN

Príkazom vo výpise (Obrázok 2.4) si môžeme zobraziť OTP pre určitého užívateľa, ktoré slúži na prevzatie a import certifikátu do web prehliadača.

```
ciscoasa(config)# crypto ca server user-db show-otp marko
Username: marko
OTP: D921675D897A34F9
Enrollment Allowed Until: 14:26:57 UTC Tue Mar 7 2017
```

Obrázok 2.5 OTP používateľa marko

Na obrázku 2.5 sú zobrazené informácie o lokálnom CA servery, ide napríklad o odtlačok certifikátu, platnosť certifikačnej autority a podobne.

```
ciscoasa(config)# sh crypto ca server

Certificate Server LOCAL-CA-SERVER:
    Status: enabled
    State: enabled
    Server's configuration is locked  (enter "shutdown" to unlock it)
    Issuer name: CN=vsb.cz
    CA certificate fingerprint/thumbprint: (MD5)
        ff0714b8 545c01c4 f7f8113a 95f95430
    CA certificate fingerprint/thumbprint: (SHA1)
        a91e1573 beff8bfa 63e07847 d0e8a71e a71330b2
    Last certificate issued serial number: 0x2
    CA certificate expiration timer: 14:26:47 UTC Nov 20 2017
    CRL NextUpdate timer: 20:26:47 UTC Feb 28 2017
    Current primary storage dir: flash:/LOCAL-CA-SERVER/

    Auto-Rollover configured, overlap period 30 days
    Autorollover timer: 14:26:46 UTC Oct 21 2017

    WARNING: Configuration has been modified and needs to be saved!!

ciscoasa(config)#
```

Obrázok 2.6 Výpis Lokálneho CA serveru

V tomto výpise (Obrázok 2.6) sú parametre užívateľa ako aj platnosť jeho certifikátu.

```
username: marko
email:    jaroslav.fiderma@gmail.com
dn:       CN=marko,OU=TAC
allowed:  14:26:57 UTC Tue Mar 7 2017
notified: 1 times
enrollment status: Enrolled, Certificate valid until 14:40:19 UTC Wed Jun 28 2017,
Renewal: Allowed
```

Obrázok 2.7 Výpis užívateľa a jeho parametre (show crypto ca server user-db)

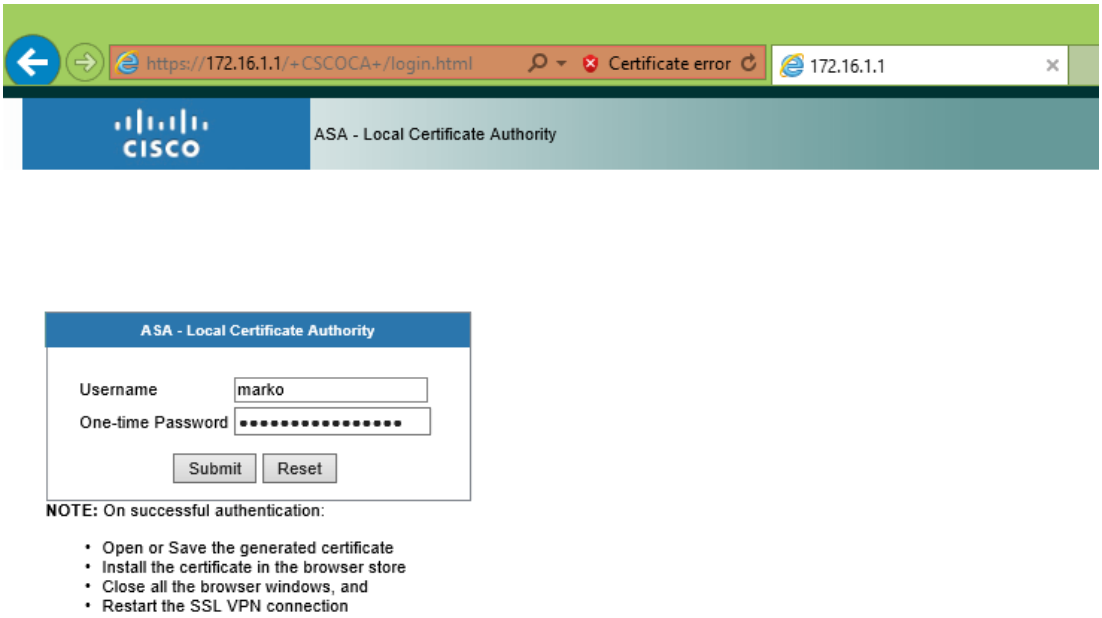
Výpis na obrázku 2.7 nám zobrazuje rôzne parametre tunela. V časti AnyConnect detailed je názov používateľa, ktorý je aktuálne prihlásený pomocou anyconnect klienta, hlási sa zo svojou IP adresou 192.168.1.2 a anyconnect klient mu priradzuje IP adresu 10.0.1.3. Anyconnect-parent je spojenie, kedy je klient vypnutý alebo odpojený a slúži k tomu aby bol po zapnutí znovu pripojený bez nutnosti autentifikácie. Čas, za ktorý sa môže takto pripojiť je definovaný na 120 minút, po uplynutí časového intervalu sa musí klient znovu verifikovať. V poslednej časti výpisu máme DTLS –Tunnel a je to spojenie kedy všetky dáta prechádzajú cez DTLS-Tunnel. Sú tu popísané všetky parametre tunela ako napríklad jeho šifrovanie, hashovanie, UDP port na obidvoch stranách a dokonca aj verzia AnyConnect klienta. Tak isto aj počet prijatých a odoslaných paketov a podobne.

```
ciscoasa(config)# show vpn-sessiondb detail anyconnect filter name marko

Session Type: AnyConnect Detailed

Username     : marko                  Index        : 2
Assigned IP  : 10.0.1.3               Public IP    : 192.168.1.2
Protocol     : AnyConnect-Parent DTLS-Tunnel
License      : AnyConnect Premium
Encryption   : AnyConnect-Parent: (1)none  DTLS-Tunnel: (1)AES128
Hashing      : AnyConnect-Parent: (1)none  DTLS-Tunnel: (1)SHA1
Bytes Tx     : 54733                  Bytes Rx     : 55515
Pkts Tx      : 68                     Pkts Rx      : 548
Pkts Tx Drop : 0                      Pkts Rx Drop : 0
Group Policy : SSL_VPN_GR             Tunnel Group : SSL_VPN_TNLGR
Login Time   : 15:17:09 UTC Tue Feb 28 2017
Duration     : 0h:17m:36s
Inactivity   : 0h:02m:46s
NAC Result   : Unknown
VLAN Mapping : N/A                    VLAN         : none

AnyConnect-Parent Tunnels: 1
DTLS-Tunnel Tunnels: 1

AnyConnect-Parent:
  Tunnel ID    : 2.1
  Public IP    : 192.168.1.2
  Encryption   : none                   Hashing      : none
  TCP Src Port : 64526                  TCP Dst Port : 443
  Auth Mode    : Certificate and userPassword
  Idle Time Out: 120 Minutes            Idle TO Left : 117 Minutes
  Client OS    : Windows
  Client Type  : AnyConnect
  Client Ver   : Cisco AnyConnect VPN Agent for Windows 4.3.02039
  Bytes Tx     : 7271                   Bytes Rx     : 795
  Pkts Tx      : 5                      Pkts Rx      : 2
  Pkts Tx Drop : 0                      Pkts Rx Drop : 0

DTLS-Tunnel:
  Tunnel ID    : 2.3
  Assigned IP  : 10.0.1.3               Public IP    : 192.168.1.2
  Encryption   : AES128                 Hashing      : SHA1
  Encapsulation: DTLSv1.0               UDP Src Port : 53976
  UDP Dst Port : 443                    Auth Mode    : Certificate and userPassword
  Idle Time Out: 120 Minutes            Idle TO Left : 117 Minutes
  Client OS    : Windows
  Client Type  : DTLS VPN Client
  Client Ver   : Cisco AnyConnect VPN Agent for Windows 4.3.02039
  Bytes Tx     : 40191                  Bytes Rx     : 54572
  Pkts Tx      : 58                     Pkts Rx      : 544
  Pkts Tx Drop : 0                      Pkts Rx Drop : 0

NAC:
  Reval Int (T): 0 Seconds              Reval Left(T): 0 Seconds
  SQ Int (T)   : 0 Seconds              EoU Age(T)   : 1072 Seconds
  Hold Left (T): 0 Seconds              Posture Token:
  Redirect URL :
```

Obrázok 2.8 Podrobný výpis parametrov VPN tunela

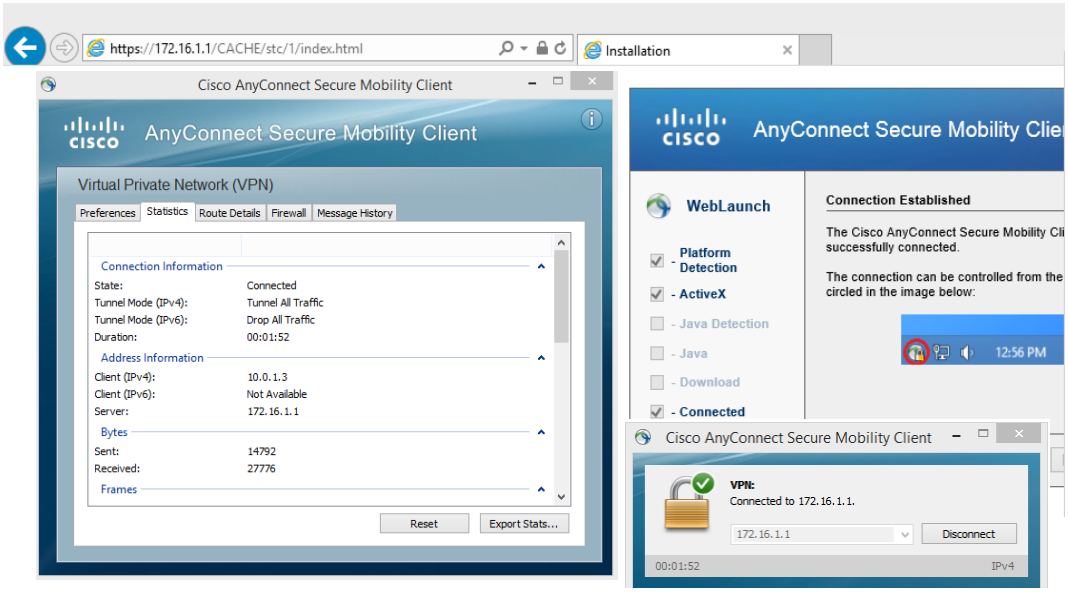
Pripojenie sa k VPN pomocou AnyConnect klienta

Prihlásenie sa pomocou užívateľského mena a OTP hesla. Po úspešnom overení si môžeme prevziať certifikát.



Obrázok 2.9 Prevzatie certifikátu

Na obrázku 2.9 máme priebeh pripojenia po úspešnej autentizácií certifikátom a po zadaní korektných prihlasovacích údajov do webového prehliadača sa automaticky nainštalujú chýbajúce aplikácie, stiahne sa AnyConnect klient a automatický sa pripojí na VPN. Informácie o VPN sa nachádzajú v rozšírenom okne AnyConnect klienta.

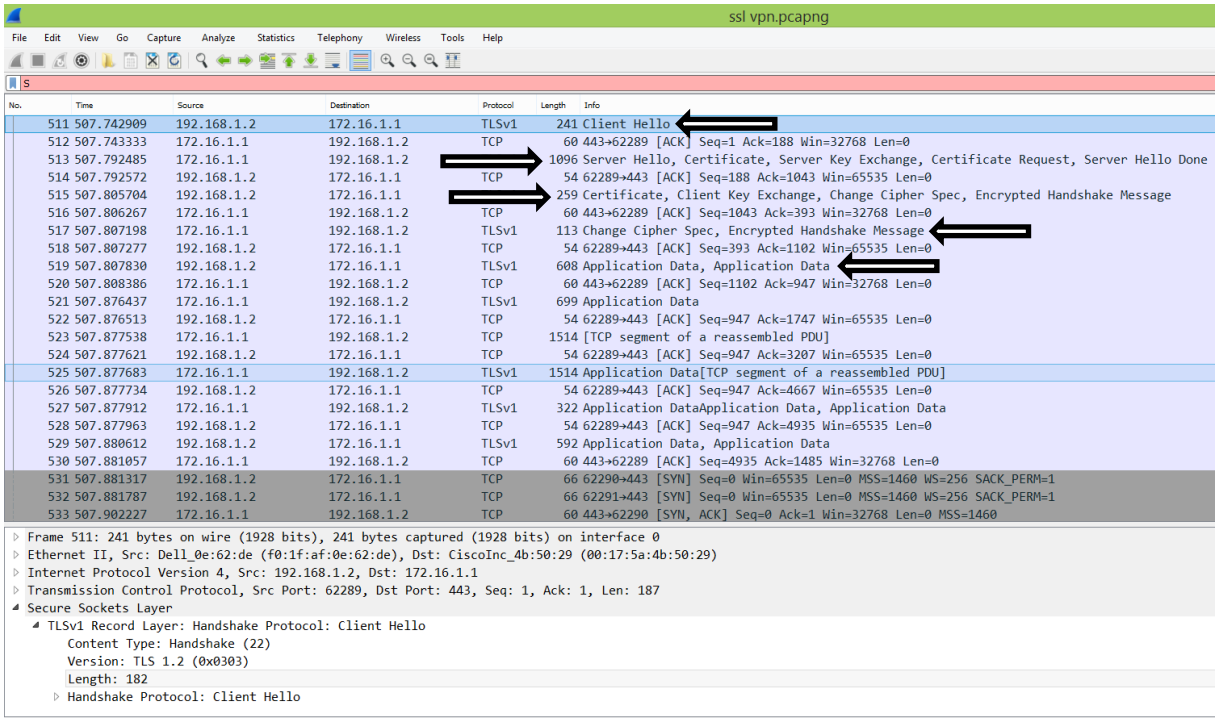


Obrázok 2.10 Pripojenie sa k VPN pomocou AnyConnect klienta

Funkčnosť VPN pripojenia môžeme otestovať pripojením sa na webový server, vytvorený na vzdialenej sieti ku ktorej sa pripájame.

Obrázok 2.11 Pripojenie sa na Web server

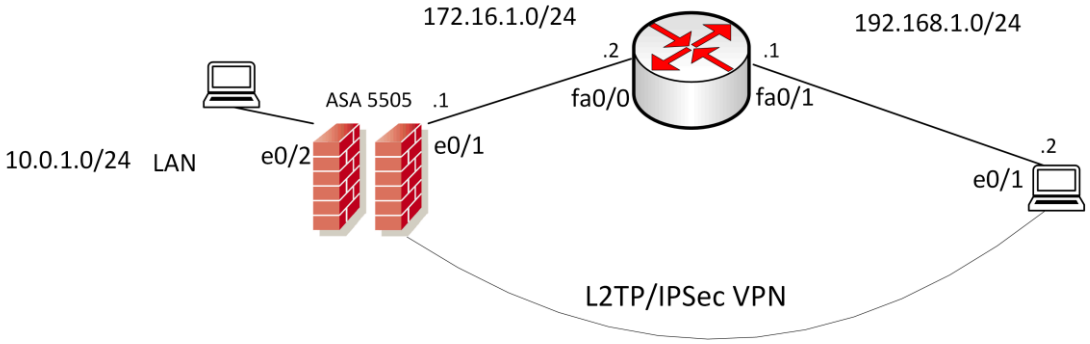
Na obrázku 2.11 vidíme výmenu správ pri zostavovaní SSL VPN spojenia, zostavovanie začína správou Hello od klienta.



Obrázok 2.12 Zachytenie SSL komunikácie pomocou programu Wireshark

2.4 Technológia L2TP/IPSec VPN

Druhá remote access VPN, ktorú sme konfigurovali je L2TP VPN. Tunel je vytváraný medzi vzdialeným zariadením a zariadením ASA. Pre zabezpečenú komunikáciu je použitý protokol IPSec. Overenie prihlasovacích údajov medzi ASA a vzdialeným zariadením je pomocou MSCHAPv2.



Obrázok 2.13 Schéma zapojenia L2TP/IPSec VPN

2.4.1 Konfigurácia L2TP over IPSEC VPN na zariadení ASA 5505

Najskôr nakonfigurujeme IPSec vo verzií IKEv1, pretože IKEv2 nepodporuje L2TP over IPSec u Cisco ASA. Ide o prvú fázu vytvorenie ISAKAMP SA, ktorá slúži na zabezpečenie výmeny informačných správ medzi peermi. V prvej fáze konfigurujeme autentifikáciu, šifrovanie a hashovanie, Diffie-Helman skupinu, životnosť SA, po ktorej sa znovu vyjednávajú parametre.

crypto ikev1 policy 1

authentication pre-share

encryption 3des

hash sha

group 2

lifetime 86400

Druhá fáza IKE SA slúži na zabezpečenie prenosu dát pomocou šifrovania a hashovania. Konfiguroval som transportný mód tunela, pretože defaultný tunelovací mód nie je podporovaný Windows L2TP/IPSec klientom. Trasnportný mód šifruje iba dáta a ponechá sa zdrojová a cieľová IP hlavička.

crypto IPSec ikev1 transform-set SECURITY esp-3des esp-sha-hmac

crypto IPSec ikev1 transform-set SECURITY mode transport

V tejto časti sme konfigurovali dynamickú crypto mapu, pretože ak chceme zostaviť VPN tunel medzi dvomi zariadeniami, musíme poznať IP adresy oboch koncov tunela. Ak nepoznáme adresu

jedného konca, pretože je dynamická, vtedy využívame dynamickú crypto mapu. VPN tunel môže byť iniciovaný iba peerom s dynamickou IP adresou, pretože druhý peer nepozná IP adresu druhého konca.

Keďže dynamická mapa nemôže byť konfigurovaná na rozhranie, tak ju prepojíme zo statickou crypto mapou a tú priradíme na vonkajšie rozhranie. V statickej crypto mape definujeme číslo 50000, ide o sekvenčné číslo, ktoré určuje prioritu danej crypto mapy. Ak máme statických a dynamických peerov s rovnakou crypto mapou, musí mať dynamická crypto mapa vyššie sekvenčné číslo (nižšiu prioritu) ako statická. V prípade, že by sme priradili vyššie sekvenčné číslo statickej crypto mape spojenie zo statickými peermi zlyhá.

crypto dynamic-map dyn_mapa 5 set ikev1 transform-set SECURITY

crypto map outside_map 50000 IPSec-isakmp dynamic dyn_mapa

crypto map outside_map interface outside

crypto ikev1 enable outside

V tomto kroku definujeme rozsah adries, ktoré budú prideľované vzdialeným VPN klientom.

ip local pool LOCALaddPOOL 10.0.1.3-10.0.1.200 mask 255.255.255.0

V tejto časti konfigurujeme parametre, ktoré budú priradené VPN klientovi a tunelovací protokol, v našom prípade *l2tp-IPSec*.

group-policy L2TPgroup internal

group-policy L2TPgroup attributes

dns-server value 8.8.8.8 4.4.4.2

vpn-tunnel-protocol l2tp-IPSec

default-domain value vsb.cz

Vytvorenie prihlasovacích údajov, ktoré slúžia na autentifikáciu na vzdialenom počítači, ide o overenie pomocou MS-CHAP protokolu, ktorý je bezpečnejší v porovnaní CHAP, pretože heslá sú šifrované.

username marko1 password dsjk59wr mschap

Vytvorenie tunnel-group, kde konfigurujeme typ tunela a jeho atribúty. V tomto prípade bol konfigurovaný východzí tunel, pretože je nastavená autentifikáciu pomocou pred-zdieľaného hesla a na strane klienta nie je možnosť definovať jeho názov. Na prepojenie *group-policy* s *tunnel-group-policy* sme použili príkaz *default-group-policy*.

tunnel-group DefaultRAGroup type remote

tunnel-group DefaultRAGroup general-attributes

address-pool LOCALaddPOOL

default-group-policy L2TPgroup

V poslednom kroku nastavíme pred-zdieľané heslo pre IKEv1 a autentifikačný protokol PPP s autentifikáciou pomocou ms-chap-v2 protokolu. Ďalej je potrebné vypnúť protokol CHAP, pretože býva štandardne zapnutý a nie je podporovaný, ak je AAA server konfigurovaný lokálne.

tunnel-group DefaultRAGroup IPSec-attributes

ikev1 pre-shared-key CqKr32Oswqfh7

tunnel-group DefaultRAGroup ppp-attributes

no authentication chap

authentication ms-chap-v2

2.4.2 Overenie konfigurácie L2TP/IPSec VPN

Na Obrázku 2.13 je prvá fáza, na ktorej vidíme IP adresu druhej strany tunela, rolu a stav na našej strane tunela.

```
ciscoasa# sh crypto ikev1 sa

IKEv1 SAs:

   Active SA: 1
    Rekey SA: 0 (A tunnel will report 1 Active and 1 Rekey SA during rekey)
Total IKE SA: 1

1   IKE Peer: 192.168.1.2
    Type    : user             Role    : responder
    Rekey   : no               State   : MM_ACTIVE
```

Obrázok 2.14 Prvá fáza IKE SA

Na Obrázku 2.14 je druhá fáza IPSec, na ktorom môžeme vidieť IP adresy lokálneho a vzdialeného konca tunela, aktuálne pripojeného klienta s prihlasovacím menom a k nemu dynamicky priradenú IP adresu z lokálneho rozsahu. Informácie o zabezpečení a podobne.

```
ciscoasa# sh crypto ipsec sa
interface: outside
    Crypto map tag: dyn_mapa, seq num: 1, local addr: 172.16.1.1

      local ident (addr/mask/prot/port): (172.16.1.1/255.255.255.255/17/1701)
      remote ident (addr/mask/prot/port): (192.168.1.2/255.255.255.255/17/1701)
      current_peer: 192.168.1.2, username: marko1
      dynamic allocated peer ip: 10.0.1.3
      dynamic allocated peer ip(ipv6): 0.0.0.0

      #pkts encaps: 25, #pkts encrypt: 25, #pkts digest: 25
      #pkts decaps: 156, #pkts decrypt: 156, #pkts verify: 156
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 25, #pkts comp failed: 0, #pkts decomp failed: 0
      #post-frag successes: 0, #post-frag failures: 0, #fragments created: 0
      #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
      #TFC rcvd: 0, #TFC sent: 0
      #Valid ICMP Errors rcvd: 0, #Invalid ICMP Errors rcvd: 0
      #send errors: 0, #recv errors: 0

      local crypto endpt.: 172.16.1.1/0, remote crypto endpt.: 192.168.1.2/0
      path mtu 1500, ipsec overhead 58(36), media mtu 1500
      PMTU time remaining (sec): 0, DF policy: copy-df
      ICMP error validation: disabled, TFC packets: disabled
      current outbound spi: F2508BF4
      current inbound spi : 8446BCBF

    inbound esp sas:
      spi: 0x8446BCBF (2219228351)
         transform: esp-3des esp-sha-hmac no compression
         in use settings ={RA, Transport, IKEv1, }
         slot: 0, conn_id: 20480, crypto-map: dyn_mapa
         sa timing: remaining key lifetime (kB/sec): (212401/3593)
         IV size: 8 bytes
         replay detection support: Y
         Anti replay bitmap:
          0x00000000 0x00000007
    outbound esp sas:
      spi: 0xF2508BF4 (4065364980)
         transform: esp-3des esp-sha-hmac no compression
         in use settings ={RA, Transport, IKEv1, }
         slot: 0, conn_id: 20480, crypto-map: dyn_mapa
         sa timing: remaining key lifetime (kB/sec): (212401/3593)
         IV size: 8 bytes
         replay detection support: Y
         Anti replay bitmap:
          0x00000000 0x00000001
```

Obrázok 2.15 Druhá fáza IPSec SA

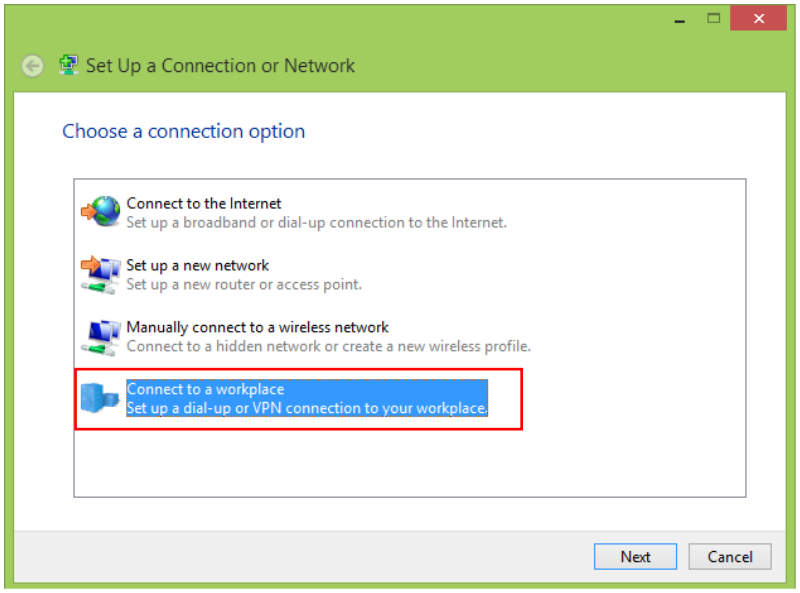
Výpis pod obrázkom zobrazuje parametre protokolov IKEv1, IPSec L2TP/IPSec. V časti IKev1 je zdrojový a cieľový UDP port, mód vyjednávania a parametre pre šifrovanie a hashovanie. V sekcií IPSec máme navyše lokálnu a vzdialenú adresu tunela, enkapsuláciu a ďalšie parametre. V poslednej časti L2TPOverIPSec nájdeme tak isto spôsob zabezpečenia, ďalšie informácie o tunely a klientovi.

```
ciscoasa(config)# show vpn-sessiondb detail ra-ikev1-ipsec filter protocol l2t$
Username     : marko1                 Index        : 5
Assigned IP  : 10.0.1.3               Public IP    : 192.168.1.2
Protocol     : IKEv1 IPsec L2TPOverIPsec
License      : Other VPN
Encryption   : IKEv1: (1)3DES  IPsec: (1)3DES  L2TPOverIPsec: (1)none
Hashing      : IKEv1: (1)SHA1  IPsec: (1)SHA1  L2TPOverIPsec: (1)none
Bytes Tx     : 2147                   Bytes Rx     : 32686
Pkts Tx      : 38                     Pkts Rx      : 264
Pkts Tx Drop : 0                      Pkts Rx Drop : 0
Group Policy : L2TPgroup              Tunnel Group : DefaultRAGroup
Login Time   : 13:24:28 UTC Tue Feb 28 2017
Duration     : 0h:10m:21s
Inactivity   : 0h:00m:00s
NAC Result   : Unknown
VLAN Mapping : N/A                    VLAN         : none

IKEv1 Tunnels: 1
IPsec Tunnels: 1
L2TPOverIPsec Tunnels: 1

IKEv1:
  Tunnel ID    : 5.1
  UDP Src Port : 500                    UDP Dst Port : 500
  IKE Neg Mode : Main                   Auth Mode    : preSharedKeys
  Encryption   : 3DES                   Hashing      : SHA1
  Rekey Int (T): 28800 Seconds          Rekey Left(T): 28179 Seconds
  D/H Group    : 2
  Filter Name  :

IPsec:
  Tunnel ID    : 5.2
  Local Addr   : 172.16.1.1/255.255.255.255/17/1701
  Remote Addr  : 192.168.1.2/255.255.255.255/17/1701
  Encryption   : 3DES                   Hashing      : SHA1
  Encapsulation: Transport
  Rekey Int (T): 3600 Seconds           Rekey Left(T): 3571 Seconds
  Rekey Int (D): 250000 K-Bytes         Rekey Left(D): 249999 K-Bytes
  Idle Time Out: 30 Minutes             Idle TO Left : 29 Minutes
  Bytes Tx     : 2147                   Bytes Rx     : 32686
  Pkts Tx      : 38                     Pkts Rx      : 264

L2TPOverIPsec:
  Tunnel ID    : 5.3
  Username     : marko1
  Assigned IP  : 10.0.1.3               Public IP    : 192.168.1.2
  Encryption   : none                   Hashing      : none
  Auth Mode    : msCHAPV2
  Idle Time Out: 30 Minutes             Idle TO Left : 29 Minutes
  Client OS    : Microsoft
  Client OS Ver: 6.3
  Bytes Tx     : 716                    Bytes Rx     : 24696
  Pkts Tx      : 19                     Pkts Rx      : 245
```

Obrázok 2.16 Podrobný výpis parametrov pre L2TP/IPSec

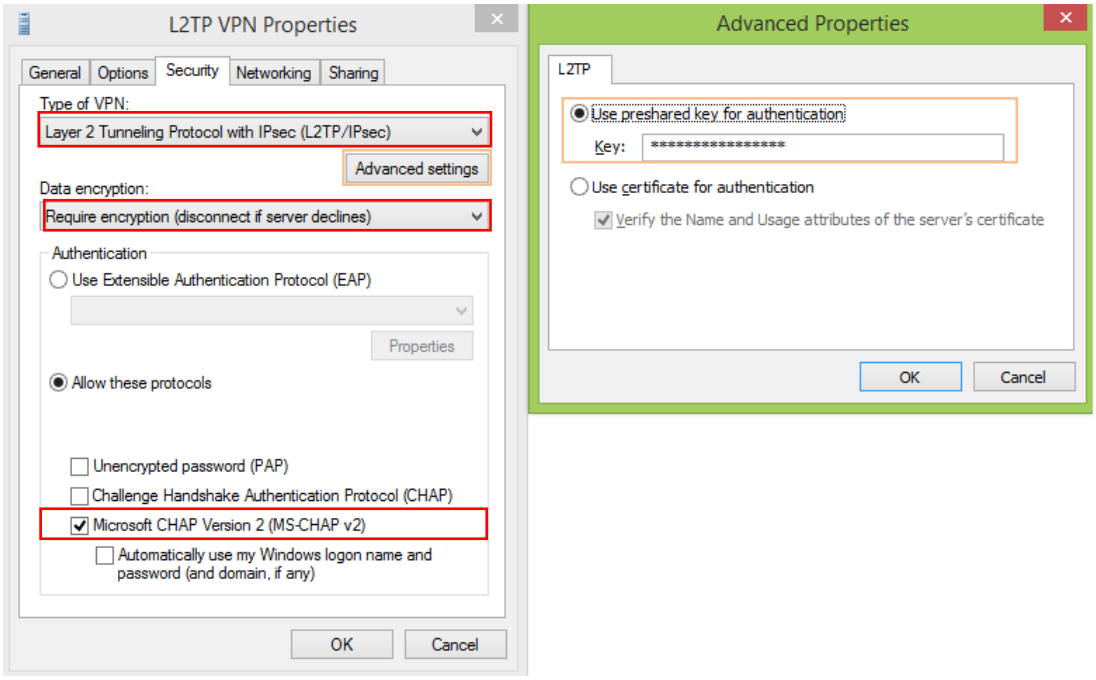
Vytvorenie a nastavenie pripojenia na klientskej strane

Prvým krokom pre vytvorenie klienta bude nastavenie VPN spojenia. Kliknutím na tlačidlo ďalej sa preklikáme k nastaveniu vzdialeného prístupu, kde zapíšeme názov pripojenia a jeho IP adresu.



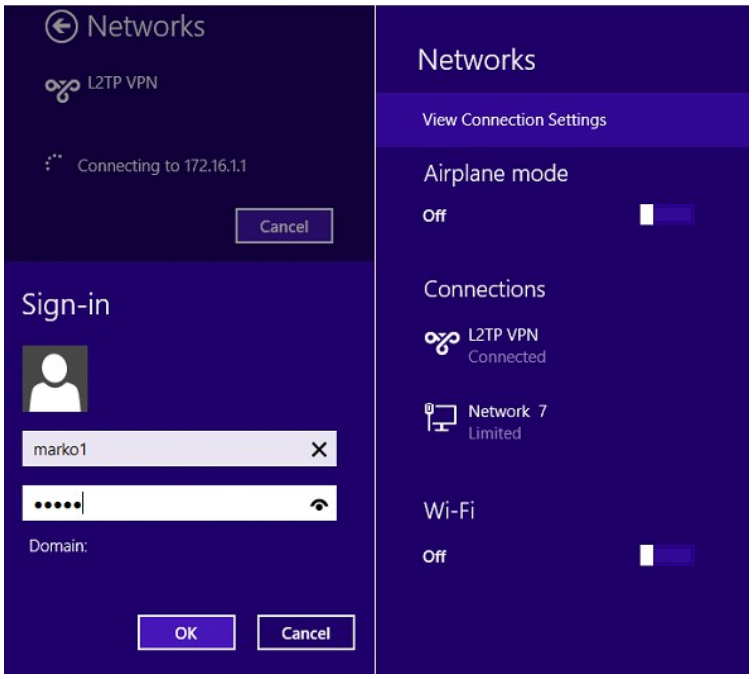
Obrázok 2.17 Vytvorenie nového pripojenia na VPN

Po úspešnom vytvorení virtuálneho sieťového rozhrania na pripojenie sa k vzdialenej sieti musíme nastaviť typ VPN, šifrovanie dát a povoliť iba MS-CHAP v2 protokol, presne tak ako je to na obrázku 2.17. V rozšírených nastaveniach potom vložíme pred-zdieľaný kľúč a potvrdíme 2 krát OK.



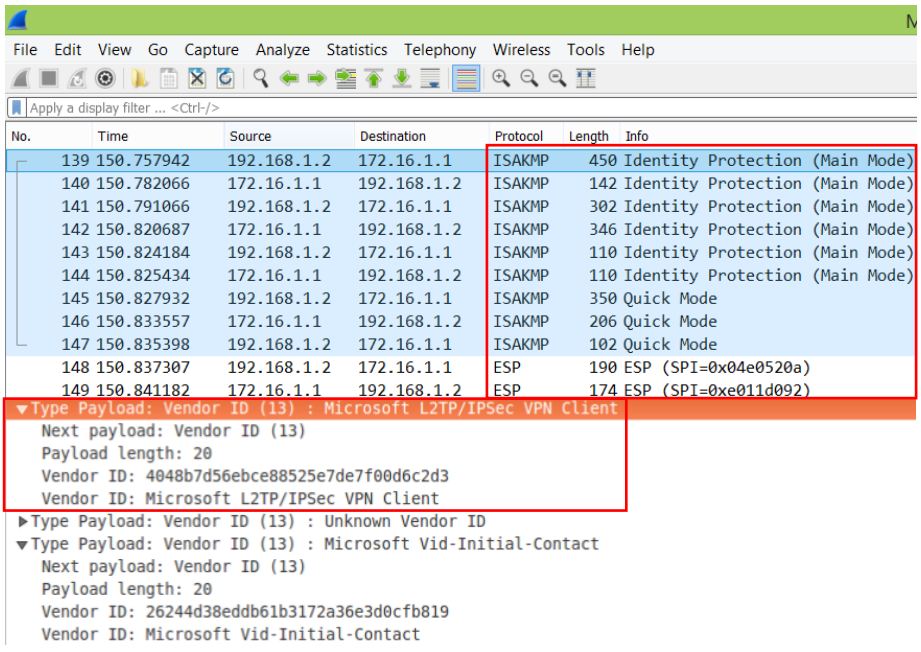
Obrázok 2.18 Nastavenie parametrov L2TP klienta

Posledným krokom je zadanie prihlasovacích údajov. Ak sme nastavili všetko správne pripojíme sa k vzdialenej sieti.



Obrázok 2.19 Zadanie prihlasovacích údajov

Na Obrázku 2.19 môžeme vidieť vytvorenie IKEv1 spojenia. Prvá fáza používa hlavný mód, druhá fáza jediný možný rýchly mód, po vyjednaní je prenos dát zabezpečený ESP hlavičkou.



Obrázok 2.20 Zachytenie komunikácie pomocou programu Wireshark

3 Porovnanie jednotlivých riešení

V tejto kapitole porovnávame VPN siete ktoré boli popísané a prakticky otestované. Jedná sa o dve VPN typu remote access a jedna typu site-to-site. Jednotlivé riešenia sme porovnávali a zhodnotili.

IPSec VPN

- Pracuje na sieťovej vrstve
- Vyžíva sa hlavne k prepojeniu dvoch pobočiek
- Blokovanie portu UDP 500 na sieťových zariadeniach, medzi peermi inicijúcimi IPSec spojenie
- Bezpečný prenos pred-zdieľaného kľúča pomocou asymetrického šifrovania
- Vyžaduje zariadenie podporujúce technológiu IPSec a jeho nastavenie
- Úroveň šifrovania prednastavená administratívne
- ESP chráni šifrovaním povodne záhlavie IP a TCP

SSL VPN

- Pracuje medzi transportnou a aplikačnou vrstvrou
- Využíva sa hlavne na pripojenie klienta k internej sieti
- Jednoduchý prístup k firemnej sieti aj cez webový prehliadač
- Používa port 443, ktorý je takmer vždy odblokovaný, teda jednoduchý prechod cez firewall
- Úroveň SSL šifrovania je väčšinou dohadovaná na najnižšom stupni (ThinClient, Clientless)
- Nie je chránené pred niektorými DoS útokmi
- DTLS vhodné pre aplikácie z citlivosťou na latenciu ako VoIP, video

L2TP/IPSec VPN

- Pracuje na linkovej vrstve
- Využíva sa hlavne na pripojenie klienta k internej sieti
- Blokovanie portu UDP 500 na sieťových zariadeniach, medzi peermi inicijúcimi IPSec spojenie
- Potreba výmeny pred-zdieľaného kľúča (IPSec)
- Nutné nastaviť virtuálne sieťové rozhranie zo špecifickými parametrami
- L2TP slúži iba na autentifikáciu klienta o bezpečnosť sa stará IPSec
- IPSec nepodporuje tunelovací mód

IPSec VPN

IPSec umožňuje preniesť hocijaký IP protokol a je dizajnovaný pre point to point spojenia medzi vzdialenými pobočkami a centrálnou pobočkou. IPSec využíva viacero protokolov, ktoré zaisťujú šifrovanie, autenticitu a integritu, zamedzujú rôznym útokom ako napríklad modifikácií alebo prečítaniu paketov pri útoku Man In The middle. IPSec tunel sa môže použiť napríklad, ak potrebujeme bezpečné prepojenie zákazníckej siete s poskytovateľom služby cez nedôveryhodnú sieť, typicky Internet. Môže ísť o pripojenie k určitým službám alebo k úložiskám ktoré zákazník využíva. IPSec poskytuje vysokú úroveň zabezpečenia ,podporuje takmer všetky používané šifrovacie a hash algoritmy. Nevýhodou môže byť zložitejšia konfigurácia IPSec VPN. IPSec je vhodné použiť pri prepájaní dvoch pobočiek alebo sieti, kde potrebujeme naozaj bezpečný prenos dát cez nezabezpečenú sieť a máme k dispozícií zariadenia podporujúce IPSec.

SSL VPN

SSL VPN je určená pre vzdialeného klienta, ktorý sa potrebuje bezpečne pripojiť k internej sieti. Vzdialeného klienta pri SSL VPN typu remote-access rozumieme, ako zariadenie napríklad počítač. Existujú 3 možnosti použitia SSL VPN, prvá z nich poskytuje pripojenie pomocou webového prehliadača s obmedzeným prístupom iba k webovým službám. Druhou možnosťou je rozšírenie webového prehliadača o služby napríklad elektronickej pošty, SSH a Telnet a poslenou možnosťou je využitie špeciálneho softwaru, nainštalovaného v mobilnom zariadení klienta, kedy hovoríme o full tunnel VPN. Výhodou SSL VPN je jednoduchosť konfigurácie na strane klienta, ktorý sa iba autentifikuje pomocou prihlasovacích údajov a môže pristupovať k internej sieti pomocou web prehliadača alebo pomocou AnyConnect klienta, ktorý sa mu automatický nainštaluje po prihlásení sa cez webové rozhranie. Ďalšou výhodou môže byť nadväzovanie spojenia prostredníctvom TCP portu 443, ktorý je štandardne povolený na väčšine sieťových zariadení. Nevýhodou môže byť nutnosť inštalácie softwaru AnyConnect klienta v prípade, že klient potrebuje prístup k protokolom na sieťovej a transportnej vrstve. Využitie tejto VPN je vo firmách, ktoré majú svoju vlastnú internú sieť a zamestnanec sa zo svojím mobilným zariadením ako klientom dokáže pripojiť do firemnej sieti z hocijakého miesta s konektivitou do Internetu.

L2TP/IPSec VPN

L2TP VPN je sama bez použitia protokolu IPSec zraniteľná, pretože je šifrovaný iba PPP rámec, pomocou MPPE šifrovania. Dátová časť paketu je síce zabezpečená a nie je možné ju prečítať, ale integrita a autenticita paketu nie je zaistená, čím môže útočník komunikáciu odpočúvať a meniť riadiace správy tunelu alebo PPP protokolu. L2TP v spojení s IPSec zaisťuje šifrovanie, autenticitu a integritu celého paketu, čim vytvára bezpečne spojenie, ktoré prechádza nedôveryhodnou sieťou. Podporovaný je iba transportný mód a ak sa spojenie vytvára s Microsoft klientom je pri L2TP/IPSec tuneli možné použiť jedine ESP hlavičku. Nevýhodou L2TP/IPSec VPN môže byť blokovanie UDP portu 500, ktorý ISAKMP používa na nadviazanie spojenia. Ďalším problémom býva NAT medzi IPSec peermi a riešením môže byť NAT-T (UDP 4500), ktorý ale nemusí byť podporovaný na všetkých zariadeniach. L2TP/IPSEC je protokol zo silnou úrovňou zabezpečenia a je vhodné ho použiť v sieťach, v ktorých nepredpokladáme blokovanie vyššie uvedených portov.

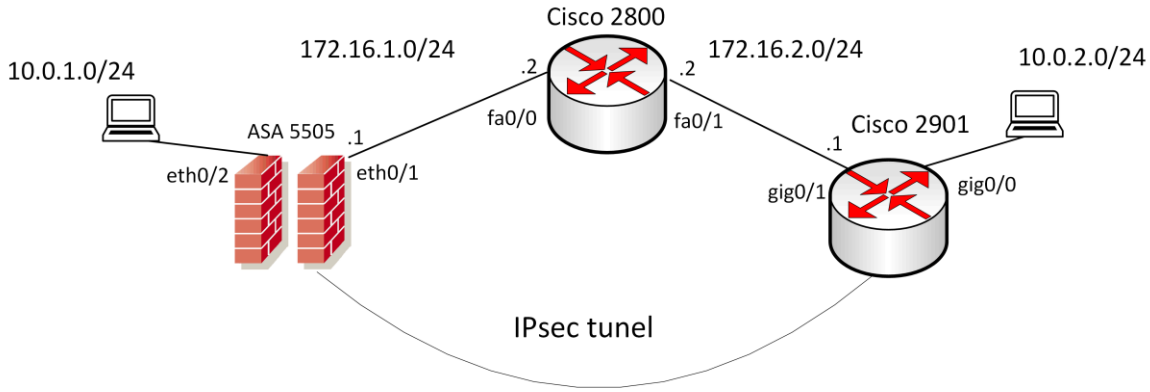
Ak teda potrebujeme priradiť prístup jednotlivo každému klientovi, výhodnejšie je použiť SSL VPN alebo L2TP/ IPSec VPN. Ak chceme priradiť homogénny prístup určitej skupine klientov alebo prepojiť dve pobočky výhodnejšie je použiť IPSec VPN.

4 Odlišnosti pri implementácií sieti VPN na zariadení ASA voči smerovaču Cisco 2901

V tejto časti sme porovnávali rozdiely vo vlastnostiach a implementácií VPN sieti medzi firewallom Cisco ASA 5505 a smerovačom Cisco 2901. Pre porovnanie sme konfigurovali rovnaké typy VPN sieti ako v predchádzajúcej kapitole 3.

4.1 Technológia IPSec VPN (IKEv2)

Návrh siete sme zvolili rovnaký ako v predchádzajúcej kapitole. IPSec spojenie sme naviazali medzi smerovačom Cisco 2901 a firewallom Cisco ASA 5505. Rozdiel v zapojení medzi smerovačom a firewallom je iba typ portov, keďže smerovač Cisco 2901 disponuje gigabitovými portami.



Obrázok 4.1 IPSec tunel medzi routrami Cisco 2901

4.1.1 Konfigurácia IPSec VPN na zariadení Cisco 2901

Na smerovači Cisco 2901 sú IP adresy priradené už štandardne na fyzické rozhrania a nie na virtuálne LAN rozhrania ako to je na zariadení Cisco ASA 5505.

V konfigurácií *crypto ikev2 proposal* definujeme návrh na zabezpečenie výmeny informačných správ medzi jednotlivými peermi. Takisto ako pri konfigurácií ASA je možné nastaviť viacero parametrov pre šifrovanie, hash a tak isto Diffie-Helman skupinu.

crypto ikev2 proposal IPSec

encryption aes-cbc-256 aes-cbc-192

integrity sha256

group 24 16 14 2

Cisco 2901 nastavuje v *crypto ikev2 policy* iba odkaz na proposal, ktoré majú byť použité pri vyjednávaní, ak by sme tento odkaz neuvideli, boli by použité východzie proposal, ktoré obsahujú všetky možnosti parametrov. ASA v tejto policy nastavuje všetky parametre pre zabezpečenú výmenu informačných správ.

crypto ikev2 policy policyIPSec

proposal IPSec

Ďalším krokom je konfigurácia *crypto ikev2 keyring,* v ktorej je nevyhnutné definovať adresu druhého konca, lokálny a vzdialený pre-shared-key, parameter peer je voliteľný. Cisco ASA definuje tieto parametre v sekcií tunnel-group.

crypto ikev2 keyring IPSec

peer ASA1

address 172.16.1.1

pre-shared-key local Jpre1-45ase

pre-shared-key remote 44ask-1dd5a

Následujúca konfigurácia *crypto ikev2 profile* obsahuje parametre, ktoré nie sú vyjednávané, ako adresa vzdialenej strany a typ autentifikácie. V tejto časti je nevyhnutné pridať odkaz na sekciu *crypto ikev2 keyring*.

crypto ikev2 profile IPSec

match identity remote address 172.16.1.1 255.255.255.255

authentication remote pre-share

authentication local pre-share

keyring local IPSec

Ekvivalentom pre konfiguráciu zabezpečenia dátového prenosu na zariadení Cisco ASA je *crypto IPSec ikev2 IPSec-proposal*, na smerovači Cisco 2901 zostal štandardne transform-set.

crypto IPSec transform-set IPSec esp-aes 192 esp-sha-hmac

mode tunnel

Všetky parametre, popisujúce IPSec tunel sú spojené pomocou *crypto map*, rovnako ako pri firewalle ASA.

crypto map IPSec 11 IPSec-isakmp

set peer 172.16.1.1

set transform-set IPSec

set ikev2-profile IPSec

match address 101

Rovnaké je aj priradenie *crypto map* na rozhranie, cez ktoré sa budú posielať IP pakety IPSec tunelom.

interface GigabitEthernet0/1

ip address 172.16.2.1 255.255.255.0

crypto map IPSec

Takisto sa rovnako nastavuje aj *access-list* na vymedzenie sieti, ktoré budú schopné komunikovať prostredníctvom zašifrovaného IPSec tunela.

access-list 101 permit ip 10.0.2.0 0.0.0.255 10.0.1.0 0.0.0.255

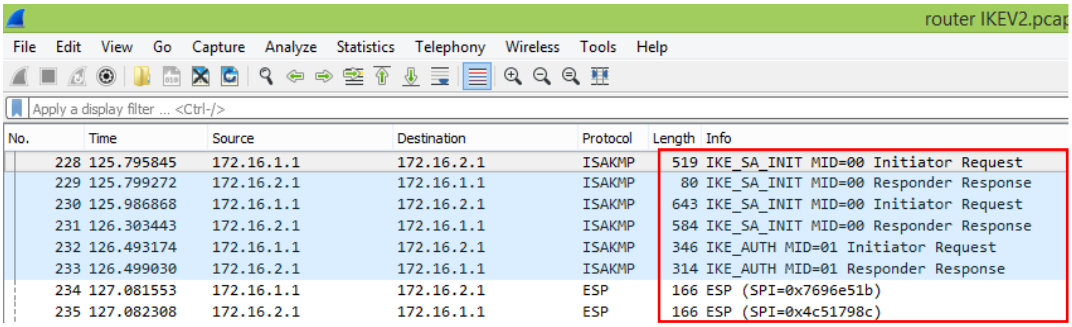
debug crypto ikev2

debug crypto ikev2 error

debug crypto ikev2 internal

4.1.2 Overenie konfigurácie IPSec VPN

Na Obrázku 4.2 je zachytená inicializácia IPSec spojenia vo verzií IKEv2 a následný prenos IP paketov šifrovaný pomocou ESP hlavičky.



Obrázok 4.2 Odchytenie komunikácie IPSec pomocou programu Wireshark

Výpisy konfigurácie sú rovnaké ako pri zariadení Cisco ASA a preto sú uvedené v prílohe.

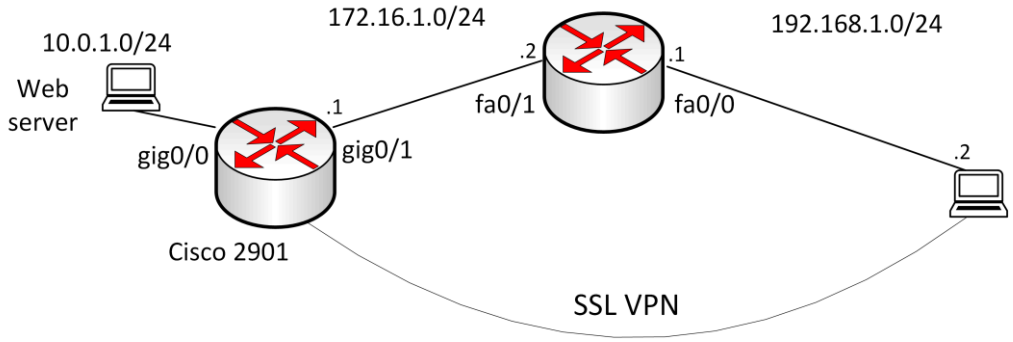
4.1.3 Porovnanie

Ak porovnávame konfiguráciu na firewalle Cisco ASA a na smerovači 2901, môžeme povedať, že na zariadení Cisco ASA je konfigurácia IPSec tunela prehľadnejšia a trochu jednoduchšia. Napríklad na smerovači je konfigurácia pre-shared-key rozdelená do dvoch sekcií pričom na firewalle máme rovnakú konfiguráciu v jednej sekcií. Firewall automaticky šifruje hesla v running-configuration, na rozdiel od smerovača, na ktorom je vhodné nastaviť šifrovanie príkazom service password-encryption.

Rozdiel vo funkcionalite a konfigurácií je, že nemôžeme nastaviť hodnotu parametra PRF, táto hodnota je zdedená od parametra integrity, avšak na zariadení Cisco ASA je tento parameter nastaviteľný, a teda v prípade, že nastavíme týmto parametrom rôzne hodnoty nenadviaže sa IPSec spojenie.

4.2 Technológia SSL VPN

Druhý návrh ktorý bol konfigurovaný a prakticky otestovaný v predchádzajúcej kapitole, je rovnaký s tým rozdielom, že namiesto firewalu Cisco ASA je použitý smerovač Cisco 2901.



Obrázok 4.3 schéma zapojenia SSL VPN

4.2.1 Konfigurácia SSL VPN na zariadení Cisco 2901

V prvej časti konfigurácie sme nastavovali autentifikáciu klienta pomocou prihlasovacích údajov uložených lokálne na smerovači. Nový model AAA umožňuje konkrétnej službe priradiť databázu, v ktorej bude hľadať prihlasovacie údaje. Na zariadení Cisco ASA konfigurujeme tieto parametre v sekcií *tunnel-group*.

aaa new-model

aaa authentication login SSLVPN local

username admin password CqW87Fd

V ďalšej časti si vygenerujeme pár RSA kľúčov. Privátny kľúč slúži na podpísanie certifikátu, verejný je distribuovaný a použitý na overenie certifikátu. Konfigurácia *crypto pki trustpoint* je v porovnaním s Cisco ASA rovnaká až na niektoré rozdiely v príkazoch. Príkaz *revocation-check none* je voliteľný a zabezpečíme ním, aby sa nevyžadovalo sledovanie stavu certifikátu.

crypto key generate rsa label RTR_AUTH modulus 1024

crypto pki trustpoint RTR_AUTH

enrollment selfsigned

fqdn ciscoasa.vsb.cz

subject-name CN=vsb.cz,CN=172.16.1.1

rsakeypair RTR_AUTH

enrollment self

revocation-check none

Konfigurácia príkazu *crypto pki enroll* zabezpečí vytvorenie certifikátu. Na smerovači sa používa architektúra PKI, ktorá umožňuje vytvárať a spravovať certifikáty, ide o novší názov pre *crypto ca*, ktorý je používaný na Cisco ASA.

crypto pki enroll RTR_AUTH

V sekcií *webvpn gateway* definujeme parametre pre nastavenie webvpn brány ako adresu a číslo portu, na ktorých bude očakávať prichádzajúce spojenie, šifrovanie, voliteľný parameter *http-redirect port 80*, ktorý presmeruje port 80 na zabezpečený port 443. Ďalej je potrebné definovať názov pre *ssl trustpoint* a aktivovať webvpn bránu.

webvpn gateway R2901_GW1

ip address 172.16.1.1 port 443

ssl encryption aes256-sha1

http-redirect port 80

ssl trustpoint RTR_AUTH

inservice

Nastavenie rozsahu adries prideľovaných klientom je rovnaké ako na Cisco ASA.

ip local pool R2901_SSLVPN 10.0.1.3 10.0.1.100

V tejto časti prepojíme nastavenia medzi *webvpn gateway*, s ktorou si klient vytvorí spojenie a *webnvpn context*, kde nastavujeme autentifikáciu, maximálny počet súčasne pripojených klientov a takisto prispôsobenie webvpn stránky, na ktorej sa klient autentifikuje.

webvpn context R2901_CONT1

gateway R2901_GW1

aaa authentication list SSLVPN

max-users 15

title "VSB-VPN"

login-message "LOGIN IN SCHOOL WEBVPN"

url-list "MyPages"

heading "MyPages"

V konfiguračnom móde *webvpn context* taktiež konfigurujeme *policy group*. Touto konfiguráciou nastavíme všetky parametre potrebné pre vytvorenie Full tunela a zabezpečíme možnosť

prevziať a inštalovať AnyConnect klienta. V prípade, že sa nepodarí nainštalovať AnyConnect klienta, príkaz *function svc-enabled* umožní klientovi využiť clientless alebo thin-client mód. Ďalšie príkazy *svc* slúžia na ponechanie softwaru AnyConnect nainštalovaného, aj keď SSL VPN spojenie nie je aktívne a vytvorenie nového tunela po obnove kľúčov.

webvpn context R2901_CONT1

policy group R2901_POLICY1

functions svc-enabled

svc keep-client-installed

svc address-pool R2901_SSLVPN netmask 255.255.255.224

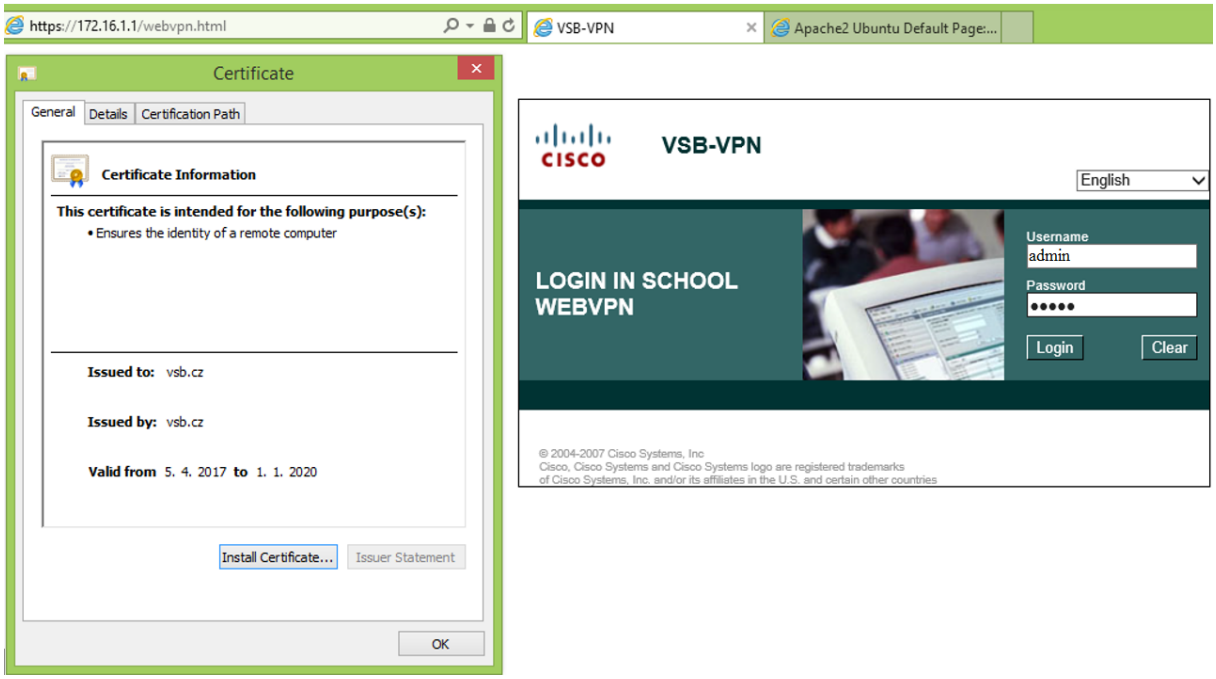
svc rekey method new-tunnel

default-group-policy R2901_POLICY1

inservice

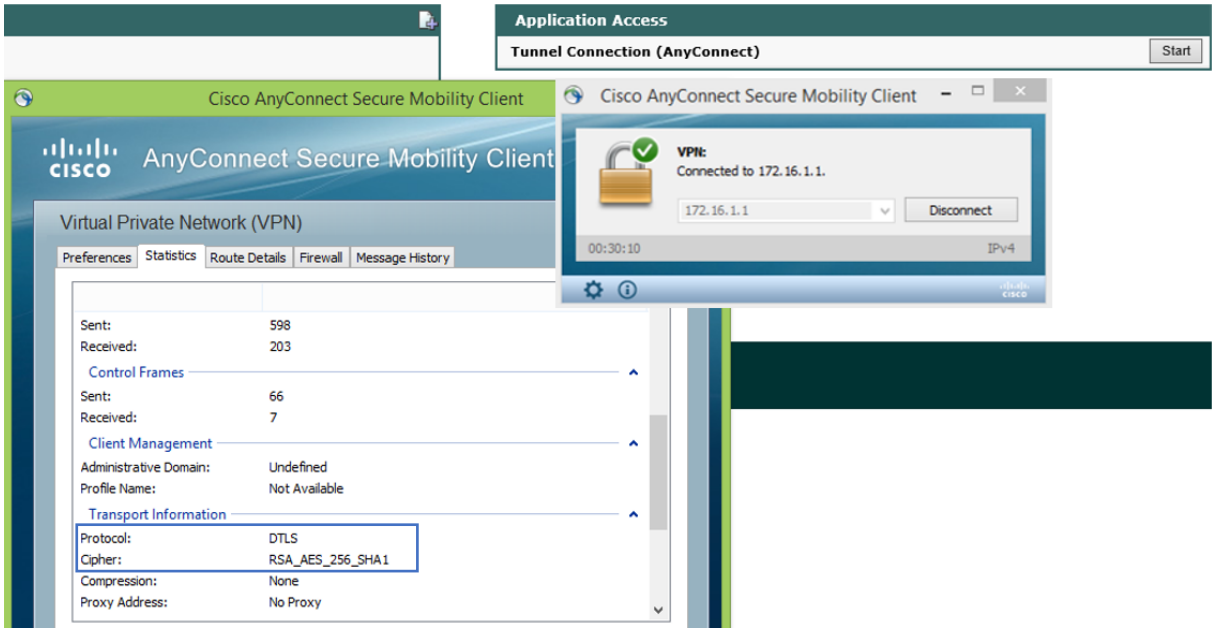
4.2.2 Overenie konfigurácie SSL VPN

Na Obrázku 4.4 je zobrazená úvodná stránka, na ktorej sa klient po úspešnej autentifikácií pripojí k internej sieti. Na ľavej strane toho obrázku môžeme vidieť certifikát, ktorý potvrdzuje identitu smerovača Cisco 2901. V porovnaní s Cisco ASA ide o iné grafické rozhranie úvodnej stránky.



Obrázok 4.4 Autentifikácia užívateľa pomocou prihlasovacích údajov

Na obrázku nižšie je klient prihlásený pomocou Cisco AnyConnect klient a dátový prenos je prenášaný DTLS tunelom.



Obrázok 4.5 Pripojenie pomocou Cisco AnyConnect klienta

Na Obrázku 4.6 je výpis konfigurácie, z ktorej môžeme vyčítať napríklad typ tunela. V našom prípade ide o Clientless a Full Tunnel, meno prihláseného používateľa a jeho IP adresa, použitá policy group a ďalšie nastavené parametre týkajúce sa tunela.

```
R2901#show webvpn session user admin context R2901_CONT1
Session Type      : Clientless
Client User-Agent : Mozilla/5.0 (Windows NT 6.3; WOW64; Trident/7.0; rv:11.0) li

Username          : admin                 Num Connection : 0
Public IP         : 192.168.1.2           VRF Name       : None
Context           : R2901_CONT1           Policy Group   : R2901_POLICY1
Last-Used         : 00:10:35              Created        : *11:53:24.611 UTC Wed Apr 5 2017
Session Timeout   : Disabled              Idle Timeout   : 2100
Citrix            : Disabled              Citrix Filter  : None
Capabilites       : svc-enabled
Session Type      : Full Tunnel
Client User-Agent : AnyConnect Windows 4.3.02039

Username          : admin                 Num Connection : 1
Public IP         : 192.168.1.2           VRF Name       : None
Context           : R2901_CONT1           Policy Group   : R2901_POLICY1
Last-Used         : 00:00:00              Created        : *11:58:48.735 UTC Wed Apr 5 2017
Session Timeout   : Disabled              Idle Timeout   : 2100
DPD GW Timeout    : 300                   DPD CL Timeout : 300
Address Pool      : R2901_SSLVPN          MTU Size       : 1399
Rekey Time        : 3600                  Rekey Method   : new-tunnel
Lease Duration    : 43200
Tunnel IP         : 10.0.1.7              Netmask        : 255.255.255.224
Tunnel-mode filte : HOST_ACL
Rx IP Packets     : 223                   Tx IP Packets  : 639
CSTP Started      : 00:32:06              Last-Received  : 00:00:00
CSTP DPD-Req sent : 0                     Virtual Access : 1
Msie-ProxyServer  : None                  Msie-PxyPolicy : Disabled
Msie-Exception    :
Client Ports      : 61262
DTLS Port         : 65528
Session Type      : Clientless
Client User-Agent : Mozilla/5.0 (Windows NT 6.3; WOW64; Trident/7.0; rv:11.0) li
```

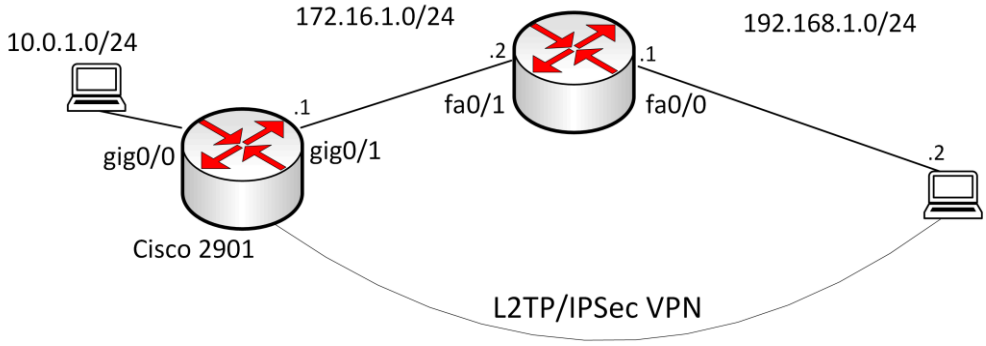
Obrázok 4.6 Výpis SSL VPN parametrov

4.2.3 Porovnanie

Ak porovnávame konfiguráciu na firewalle Cisco ASA a na smerovači Cisco 2901, z hľadiska syntaxe ide o iné názvy jednotlivých sekcií a iné názvy pre jednotlivé príkazy. Z hľadiska funkcionality Cisco smerovač síce podporuje súčasné overenie pomocou prihlasovacích údajov a certifikátu, ale nepodporuje odovzdanie lokálne uloženého certifikátu pomocou https protokolu. Ak by sme teda chceli overenie klienta pomocou certifikátu pred prihlásením bolo by možné napríklad vygenerovať certifikát priamo do príkazového riadku smerovača, čo by bolo pre testovacie účely praktizovateľné, ale v praxi nerealizovateľné. Ďalšou, už realizovateľnou možnosťou aj v praxi by bolo vytvorenie externého autentifikačného servera, ktorý by generoval certifikát a klient by si ho bol schopný prevziať pomocou https protokolu, podobne ako pri konfigurácií na Cisco ASA

4.3 Technológia L2TP/IPSec VPN

Topológia je rovnaká ako pri zapojení s firewallom ASA, jediným rozdielom je, smerovač 2901, ktorý nám bude slúžiť ako VPN brána alebo koncentrátor.



Obrázok 4.7 Schéma zapojenia L2TP/IPSec VPN

4.3.1 Konfigurácia L2TP/IPSec na zariadení Cisco 2901

Na začiatok nastavíme PPP autentifikáciu pomocou lokálne nakonfigurovaných prihlasovacích údajov, rovnako ako v predchadzajúcej podkapitole.

aaa new-model

aaa authentication ppp PPP_AUTH local

username admin password *CqW87Fd*

V tomto kroku povoľujeme prichádzajúce L2TP spojenie, takisto definujeme virtuálne rozhranie, z ktorého sa bude spojenie zostavovať. Na zariadení Cisco ASA nie je potrebné konfigurovať komutovaný prístup VPDN a protokol L2TP/IPSec povoľujeme sekcií *group-policy*.

vpdn enable

vpdn-group L2TP

accept-dialin

protocol l2tp

virtual-template 2

no l2tp tunnel authentication

Konfigurácia prvej fázy IPSec je rovnaká ako na zariadení Cisco ASA, odlišuje sa iba názov sekcie, ktorý ma názov *crypto ikev1 policy*.

crypto isakmp policy 1

encr 3des

hash sha

authentication pre-share

group 2

lifetime 86400

V tomto kroku nastavujeme pred-zdieľaný kľúč pre dynamicky sa pripájajúcich klientov, ktorí môžu mať každými prihlásením inú IP adresu. Na Cisco ASA sa tento príkaz nepoužíva a konfigurácia je rozdelená do dynamickej crypto mapy a sekcie *tunnel-group*.

crypto isakmp key Pda7M@9w4x address 0.0.0.0 0.0.0.0

Nastavenie druhej fázy na smerovači presne korešponduje s nastavením na Cisco ASA.

crypto IPSec transform-set L2TP_IPSEC esp-3des esp-sha-hmac

mode transport

Konfigurácia dynamickej krypto mapy je rovnaká ako na firewalle ASA.

crypto dynamic-map dyn-map 10

set transform-set L2TP_IPSEC

crypto map L2TP_TUNNEL 65500 IPSec-isakmp dynamic dyn-map

Cisco ASA neaplikuje *crypto map* na rozhraní ako Cisco smerovač, ale v globálnom konfiguračnom režime.

interface GigabitEthernet0/1

ip address 172.16.1.1 255.255.255.0

crypto map L2TP_TUNNEL

Rozhranie *Virtual-Template* predstavuje akúsi šablónu, ktorá je určená pre nastavenie rozhraní. Tieto rozhrania sú dynamicky vytvárané VPDN serverom pre každého pripojeného klienta osobitne.

interface Virtual-Template 2

ip unnumbered gig0/1

peer default ip address pool L2TP_CLIENT_POOL

ppp authentication ms-chap-v2 PPP_AUTH

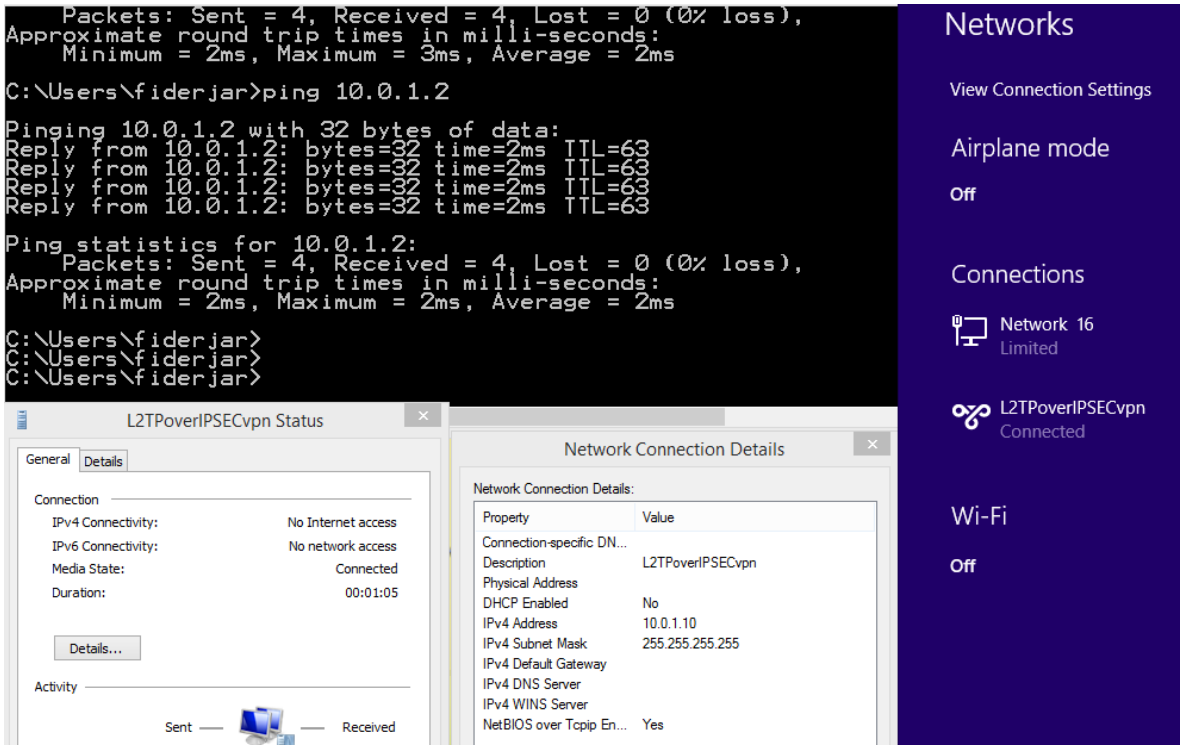
Nastavenie rozsahu IP adries, ktoré budú priradené VPN klientom je rovnaké ako na firewalle ASA. V prípade konfigurácie statickej cesty ide iba o inú syntax.

ip local pool L2TP_CLIENT_POOL 10.0.1.3 10.0.1.10

ip route 192.168.1.0 255.255.255.0 172.16.1.2

4.3.2 Overenie konfigurácie L2TP/IPSec VPN

Na obrázku 4.8 je posielaný ping zo zariadenia pripojeného k VPN na zariadenie v internej sieti. Ďalej si môžeme všimnúť, že klient pripájajúci sa k VPN sieti dostáva pridelenú IP adresu z vopred definovaného rozsahu.



Obrázok 4.8 Klient pripojený k VPN, overenie pingom

Na obrázku 4.9 je výpis, na ktorom vidíme základné informácie o vytvorenom L2TP/IPSec spojení, informácie o virtuálnom rozhraní Vi2.1, pripojeného klienta a jeho IP adresu.

```
L2TP#sh vpdn

L2TP Tunnel and Session Information Total tunnels 1 sessions 1

LocTunID    RemTunID    Remote Name    State  Remote Address  Sessn L2TP Class/
                                                              Count VPDN Group
52739       5           WL300019.eu.t est    192.168.1.2     1     L2TP_VPN

LocID       RemID       TunID       Username, Intf/      State  Last Chg Uniq ID
                                    Vcid, Circuit
24666       1           52739       admin, Vi2.1         est    00:00:15 10
```

Obrázok 4.9 Zobrazenie L2TP spojenia

4.3.3 Porovnanie

Porovnanie konfigurácie na smerovači a na firewale Cisco ASA z hľadiska syntaxe ide tak isto ako pri SSL VPN o dosť odlišnú konfiguráciu, rovnaká syntax je iba pri konfigurácií dynamickej mapy a prvej fázy IPSec. Navyše konfigurujeme komutovaný prístup VPDN a virtual-tamplate, čo na Cisco ASA konfigurujeme v sekcií tunnel group spolu s autentizáciou. Autentizácia sa na smerovači konfiguruje pomocou architektúry AAA. Funkcionalita je rovnaká ako na firewale Cisco ASA. Na smerovači je konfigurácia zložitejšia a chýba aj výpis show vpn-sessiondb, ktorý zobrazuje detailne informácie IPSec aj L2TP/IPSec tunela.

4.4 Porovnanie Cisco ASA 5505 a Cisco 2901

Zo zariadením Cisco ASA 5505 sa mi v porovnaní zo smerovačom Cisco 2901 pracovalo lepšie, rozdiel bol napríklad vo vynechaní príkazu *do* v konfiguračnom móde v porovnaní zo smerovačom, kde je tento príkaz nutné použiť. Na smerovači mi chýbal príkaz *show vpn-sessiondb,* ktorý zobrazuje prehľadný výpis nakonfigurovaného tunela. Keďže ide o firewall, heslá boli šifrované, ale na testovanom smerovači bolo v tomto prípade nutné zadať príkaz *service-password encryption*. Ďalej je možnosť zobraziť sekciu, napríklad prvej fázy IPSec pomocou príkazu *show running-config crypto isakmp* a podobne aj druhej fázy výmenou isakmp za *IPSec*.

Záver

V prvej kapitole som rozoberal jednotlivé typy virtuálnych privátnych sieti z hľadiska prepojenia, ich bezpečnostné parametre a konkrétne reálne používané technológie. Prvou popisovanou technológiou je IPSec VPN, ktorá poskytuje viacero spôsobov, ktorými chráni dáta pred útočníkom a používa sa hlavne ako site-to-site VPN. V tejto kapitole sú ďalej spomenuté taktiež veľmi bezpečné spôsoby pripojenia sa k privátnym sieťam ako SSL VPN a L2TP/IPSec, ktoré sú na rozdiel od IPSec VPN využívané ako remote access VPN a slúžia na pripojenie klienta k firemnej sieti.

Druhá kapitola je praktickou časťou, v ktorej som sa zaoberal návrhom a implementáciou troch druhov VPN, ktoré teoreticky popisujeme v prvej kapitole. Na začiatku tejto kapitoly je krátky popis funkcií a vlastnosti firewalu Cisco ASA 5505 spolu s virtuálnymi privátnymi sieťami, ktoré toto zariadenie podporuje a ktoré sú aj ďalej konfigurované. V prvom návrhu IPSec VPN bola použitá najnovšia verzia IKEv2, ktorá sa od IKEv1 odlišuje inou výmenou správ alebo možnosťou navoliť viacero možnosti šifrovania, hashovania a Diffi-helman skupiny, ktoré budú vyjednávané. Ďalej bola implementovaná funkcia vloženia statickej cesty klienta pripojeného v privátnej sieti do smerovacej tabuľky prostredníctvom IPSec tunela RRI. Druhým realizovaným tunelom je SSL VPN v móde full tunnel, s využitím dvojfaktorovej autentizácie a posledná realizovaná VPN je L2TP/IPSec, kde ide o L2TP VPN, ktorá je zabezpečená pomocou IPSec.

V ďalšej kapitole som zhodnotil všetky tri realizované VPN a to bodovým porovnaním a celkovým zhodnotením, nájdeme tam rozdiely medzi jednotlivými VPN, porovnávané výhody, nevýhody a možnosti použitia v praxi.

Posledná kapitola je druhou praktickou časťou, v ktorej som konfiguroval už spomenuté VPN na smerovači Cisco 2901. Ďalej sme porovnávali rozdiely v implementácií a funkcionalite medzi jednotlivými VPN konfigurovanými na firewale Cisco ASA a na smerovači Cisco 2901. Hlavné rozdiely medzi zariadeniami Cisco ASA a Cisco 2901 boli v konfigurácií SSL VPN a L2TP VPN. Odlišnosti boli aj pri IPSec VPN, ale nie tak významné ako pri predchádzajúcich dvoch VPN. Vo funkcionalite boli rozdiely iba pri použití dvojfaktorového overenia u SSL VPN, kedy Cisco smerovač 2901 nepodporoval export vlastného certifikátu pomocou HTTP.

V diplomovej práci som pracoval s troma odlišnými typmi VPN sieti, ktoré majú v praxi veľké využitie. Pri každej z technológií som popísal ich vlastnosti a fungovanie. Ďalej som navrhol zapojenia a otestoval konfiguráciu všetkých popísaných technológií na zariadení Cisco ASA 5505. Posledným krokom bolo porovnanie rozdielov vo funkcionalite a konfigurácií zo smerovačom Cisco 2901. Pri konfigurácií sa vyskytlo viacero problémov, či už s nenadviazaním spojenia pri IPSec VPN alebo pri inštalácií dôveryhodného certifikátu a podobne. Preto som každú časť konfigurácie opísal a takisto upozornil na niektoré príkazy, pri ktorých sa môže užívateľ pri konfigurácií dopustiť chyby. Pri riešení problémov som používal rôzne debugovacie príkazy, ktoré môžete nájsť v použitej literatúre [14] [15].

Ďalším pokračovaním práce, by mohla byť konfigurácia PPTP VPN na firewalle a jej následné porovnanie s konfiguráciou na smerovači. Navyše by sme mohli otestovať rôzne funkcie, ktoré jednotlivé VPN technológie umožňujú alebo nastavenie týchto VPN pomocou grafického rozhrania ASDM na firewalle Cisco ASA 5505.

Použitá literatúra

[1] FRAHIM, Jazib. Cisco Asa: all-in-one next-generation firewall, IPS, and VPN services. 3rd Ed. Indianapolis, IN: Cisco Press, 2014 ISBN 9781587143076.

[2] User Guide for Cisco Security Manager 4.1 [online]. [cit. 2016-10-05]. Dostupné z: http://www.cisco.com/c/en/us/td/docs/security/security_management/cisco_security_manager/security_manager/4-1/user/guide/CSMUserGuide_wrapper/vpIPSec.html

[3] VPN 1 - IPSec VPN a Cisco [online]. [cit. 2016-3-05]. Dostupné z: http://www.samuraj-cz.com/clanek/vpn-1-IPSec-vpn-a-cisco/

[4] VPN 2 - Úvod do Cisco ASA a možnosti VPN [online]. [cit. 2016-3-06]. Dostupné z: http://www.samuraj-cz.com/clanek/vpn-2-uvod-do-cisco-asa-a-moznosti-vpn/

[5] VPN 4 - Konfigurace Cisco Clientless SSL VPN na Cisco ASA [online]. [cit. 2016-3-06]. Dostupné z: http://www.samuraj-cz.com/clanek/vpn-4-konfigurace-cisco-clientless-ssl-vpn-na-cisco-asa/

[6] Jak funguje IPSEC ? [online]. [cit. 2016-4-12]. Dostupné z: http://www.security-portal.cz/clanky/jak-funguje-IPSec

[7] VPNs and VPN Technologies [online]. [cit. 2016-4-14]. Dostupné z: http://www.ciscopress.com/articles/article.asp?p=24833&seqNum=6

[8] How IPSec Works [online]. [cit. 2016-4-14]. Dostupné z: https://technet.microsoft.com/en-us/library/cc759130(v=ws.10).aspx

[9] MACHNÍK, Petr. Širokopásmové sítě pro integrovanou výuku VUT a VŠB-TUO [online]. [cit. 2016-4-12]. Dostupné po prihlásení sa na moodle: https://comtech.vsb.cz/moodle/pluginfile.php/2361/mod_resource/content/4/%C5%A0irokop%C3%A1smov%C3%A9%20s%C3%ADt%C4%9B.pdf

[10] IKEv2 Phase 1 (IKE SA) and Phase 2 (Child SA) Message Exchanges. [online]. [cit. 2016-4-14]. Dostupné z: http://www.omnisecu.com/tcpip/ikev2-phase-1-and-phase-2-message-exchanges.php

[11] How TLS/SSL Works. [online]. [cit. 2016-4-14]. Dostupné z: https://technet.microsoft.com/en-us/library/cc783349(v=ws.10).aspx

[12] HUDEC, Ladislav Bezpečnostné brány [online]. [cit. 2016-4-16]. Dostupné z: http://www2.fiit.stuba.sk/~lhudec/CS/9_prednaska.ppt

[13] ASA 5505 Viso Stencil [online]. [cit. 2017-1-15]. Dostupné z: https://supportforums.cisco.com/discussion/10742166/asa-5505-viso-stencil

[14] Site-to-Site IKEv2 Tunnel between ASA and Router Configuration Examples [online]. [cit. 2017-3-15]. Dostupné z: http://www.cisco.com/c/en/us/support/docs/security-vpn/IPSec-negotiation-ike-protocols/117337-config-asa-router-00.html#anc23

[15] SSL VPN [online]. [cit. 2017-3-22]. Dostupné z: http://www.cisco.com/c/en/us/td/docs/ios/12_4t/12_4t11/htwebvpn.html#wp1058483

Zoznam príloh

Príloha A: *IPSec VPN Cisco ASA 5505 – skrátený výpis konfigurácie*

```
hostname ASA1
!
interface Ethernet0/1
 switchport access vlan 2
!
interface Ethernet0/2
 switchport access vlan 3
!
interface Vlan2
 nameif OUTSIDE
 security-level 0
 ip address 172.16.1.1 255.255.255.0
!
interface Vlan3
 nameif INSIDE
 security-level 100
 ip address 10.0.1.1 255.255.255.0
!
access-list 101 extended permit ip 10.0.1.0 255.255.255.0 10.0.2.0 255.255.255.
!
route OUTSIDE 0.0.0.0 0.0.0.0 172.16.1.2 1
!
crypto IPSec ikev2 IPSec-proposal VPNZAB
 protocol esp encryption aes-192
 protocol esp integrity sha-1
crypto IPSec security-association pmtu-aging infinite
crypto map TrafficSP 1 match address 101
crypto map TrafficSP 1 set peer 172.16.2.1
crypto map TrafficSP 1 set ikev2 IPSec-proposal VPNZAB
crypto map TrafficSP 1 set reverse-route
```

```
crypto map TrafficSP interface OUTSIDE
crypto ikev2 policy 1
 encryption aes-192
 integrity sha512 sha256
 group 19 14 5
 prf sha256 sha
crypto ikev2 enable OUTSIDE
tunnel-group 172.16.2.1 type IPSec-l2l
tunnel-group 172.16.2.1 IPSec-attributes
 ikev2 remote-authentication pre-shared-key *****
 ikev2 local-authentication pre-shared-key *****
!
policy-map global_policy
 class inspection_default
  inspect icmp
: end
```

Príloha B: *IPSec VPN Cisco ASA 5505 – skrátený výpis konfigurácie*

```
hostname ASA2
interface Ethernet0/1
 switchport access vlan 2
!
interface Ethernet0/2
 switchport access vlan 3
!
interface Vlan2
 nameif OUTSIDE
 security-level 0
 ip address 172.16.2.1 255.255.255.0
!
interface Vlan3
 nameif INSIDE
 security-level 100
 ip address 10.0.2.1 255.255.255.0
!
access-list 101 extended permit ip 10.0.2.0 255.255.255.0 10.0.1.0 255.255.255.
route OUTSIDE 0.0.0.0 0.0.0.0 172.16.2.2 1
!
crypto IPSec ikev2 IPSec-proposal VPNZAB
 protocol esp encryption aes-192 aes
 protocol esp integrity sha-1
crypto IPSec security-association pmtu-aging infinite
crypto map TrafficSP 1 match address 101
crypto map TrafficSP 1 set peer 172.16.1.1
crypto map TrafficSP 1 set ikev2 IPSec-proposal VPNZAB
crypto map TrafficSP interface OUTSIDE
!
crypto ikev2 policy 1
```

```
 encryption aes-256 aes-192
 integrity sha512
 group 21 24 14 2
 prf sha512 sha256 sha
!
crypto ikev2 enable OUTSIDE
tunnel-group 172.16.1.1 type IPSec-l2l
tunnel-group 172.16.1.1 IPSec-attributes
 ikev2 remote-authentication pre-shared-key *****
 ikev2 local-authentication pre-shared-key *****
!
policy-map global_policy
 class inspection_default
  inspect icmp
: end
```

Príloha C: *SSL VPN Cisco ASA 5505 – skrátený výpis konfigurácie*

```
ip local pool VPN_Pool 10.0.1.3-10.0.1.200 mask 255.255.255.0
!
interface Ethernet0/1
 switchport access vlan 2
!
interface Ethernet0/2
 switchport access vlan 3
!
interface Vlan2
 nameif outside
 security-level 0
 ip address 172.16.1.1 255.255.255.0
!
interface Vlan3
 nameif inside
 security-level 100
 ip address 10.0.1.1 255.255.255.0
!
route outside 192.168.1.0 255.255.255.0 172.16.1.2 1
crypto ca trustpoint LOCAL-CA-SERVER
 keypair LOCAL-CA-SERVER
 crl configure
crypto ca trustpoint IdentityCert
 enrollment self
 subject-name CN=vsb.cz,CN=172.16.1.1
 keypair LOCAL-CA-SERVER
!
crypto ca server
 lifetime ca-certificate 265
 lifetime certificate 120
```

```
 OTP expiration 168
 keysize 2048
 subject-name-default CN=vsb.cz
 issuer-name CN=vsb.cz
!
ssl trust-point IdentityCert outside
webvpn
 enable outside
 anyconnect image disk0:/any.pkg 1
 anyconnect enable
 tunnel-group-list enable
group-policy SSL_VPN_GR internal
group-policy SSL_VPN_GR attributes
 wins-server none
 dns-server none
 vpn-simultaneous-logins 30
 vpn-idle-timeout 120
 vpn-tunnel-protocol ssl-client
!
username marko password JwUcQSm75Ei3j8C0 encrypted
tunnel-group SSL_VPN_TNLGR type remote-access
tunnel-group SSL_VPN_TNLGR general-attributes
 address-pool VPN_Pool
 default-group-policy SSL_VPN_GR
!
tunnel-group SSL_VPN_TNLGR webvpn-attributes
 authentication aaa certificate
 group-alias SSL_VPN_TNLGR enable
!
policy-map global_policy
 class inspection_default
  inspect icmp
```

Príloha D: *L2TP/IPSec VPN Cisco ASA 5505 – skrátený výpis konfigurácie*

```
hostname ciscoasa
ip local pool Address-pool 10.0.0.3-10.0.0.200 mask 255.255.255.0
!
interface Ethernet0/1
 switchport access vlan 2
!
interface Ethernet0/2
switchport access vlan 3
 shutdown
!
interface Vlan2
 nameif outside
 security-level 0
 ip address 172.16.1.1 255.255.255.0
!
interface Vlan3
 nameif inside
 security-level 100
 ip address 10.0.1.1 255.255.255.0
!
crypto IPSec ikev1 transform-set SECURITY esp-3des esp-sha-hmac
crypto IPSec ikev1 transform-set SECURITY mode transport
crypto dynamic-map dyn_mapa 5 set ikev1 transform-set SECURITY
crypto map outside_map 50000 IPSec-isakmp dynamic dyn_mapa
crypto map outside_map interface outside
crypto ikev1 enable outside
!
crypto ikev1 policy 1
 authentication pre-share
 encryption 3des
 hash sha
```

```
 group 2
 lifetime 86400
!
group-policy DefaultRAGroup internal
group-policy DefaultRAGroup attributes
group-policy L2TP-VPN internal
group-policy L2TP-VPN attributes
 dns-server value 8.8.8.8 4.4.4.2
 vpn-tunnel-protocol l2tp-IPSec
 default-domain value vsb.cz
!
username marko1 password f3UhLvUj1QsXsuK7 encrypted
!
tunnel-group DefaultRAGroup general-attributes
 address-pool Address-pool
 default-group-policy L2TP-VPN
tunnel-group DefaultRAGroup IPSec-attributes
 ikev1 pre-shared-key *****
tunnel-group DefaultRAGroup ppp-attributes
 no authentication chap
 authentication ms-chap-v2
class inspection_default
  inspect icmp
: end
```

Príloha E: *IPSec VPN Cisco 2901 – skrátený výpis konfigurácie*

```
hostname R2TNL
no aaa new-model
!
crypto ikev2 proposal IPSec
 encryption aes-cbc-256 aes-cbc-192
 integrity sha256
 group 24 16 14 2
!
crypto ikev2 policy policyIPSec
 proposal IPSec
!
crypto ikev2 keyring IPSec
 peer ASA1
  address 172.16.1.1
  pre-shared-key local S$vS3e9TD-Q
  pre-shared-key remote kI4rq5asE-W
!
crypto ikev2 profile IPSec
 match identity remote address 172.16.1.1 255.255.255.255
 authentication remote pre-share
 authentication local pre-share
 keyring local IPSec
!
crypto IPSec transform-set IPSec esp-aes 192 esp-sha-hmac
 mode tunnel
!
crypto map IPSec 11 IPSec-isakmp
 set peer 172.16.1.1
 set transform-set IPSec
```

```
 set ikev2-profile IPSec
 match address 101
!
interface GigabitEthernet0/0
 ip address 10.0.2.1 255.255.255.0
 duplex auto
 speed auto
!
interface GigabitEthernet0/1
 ip address 172.16.2.1 255.255.255.0
 duplex auto
 speed auto
 crypto map IPSec
ip route 0.0.0.0 0.0.0.0 172.16.2.2
!
access-list 101 permit ip 10.0.2.0 0.0.0.255 10.0.1.0 0.0.0.255
end
```

Príloha F: *IPSec VPN Cisco ASA 5505 – skrátený výpis konfigurácie*

```
hostname ASA1
!
interface Ethernet0/1
 switchport access vlan 2
!
interface Ethernet0/2
 switchport access vlan 3
!
interface Vlan2
 nameif OUTSIDE
 security-level 0
 ip address 172.16.1.1 255.255.255.0
!
interface Vlan3
 nameif INSIDE
 security-level 100
 ip address 10.0.1.1 255.255.255.0
!
access-list 101 extended permit ip 10.0.1.0 255.255.255.0 10.0.2.0 255.255.255.0
!
route OUTSIDE 0.0.0.0 0.0.0.0 172.16.1.2 1
!
crypto IPSec ikev2 IPSec-proposal VPNZAB
 protocol esp encryption aes-256 aes-192
 protocol esp integrity sha-1
!
crypto IPSec security-association pmtu-aging infinite
crypto map TrafficSP 1 match address 101
crypto map TrafficSP 1 set peer 172.16.2.1
```

```
crypto map TrafficSP 1 set ikev2 IPSec-proposal VPNZAB
crypto map TrafficSP 1 set reverse-route
crypto map TrafficSP interface OUTSIDE
!
crypto ikev2 policy 1
 encryption aes-256
 integrity sha256
 group 21 20 14
 prf sha256
crypto ikev2 enable OUTSIDE
!
tunnel-group 172.16.2.1 type IPSec-l2l
tunnel-group 172.16.2.1 IPSec-attributes
 ikev2 remote-authentication pre-shared-key *****
 ikev2 local-authentication pre-shared-key *****
!
policy-map global_policy
 class inspection_default
 inspect icmp
!
: end
```

Príloha G: *SSL VPN Cisco 2901 – skrátený výpis konfigurácie*

```
hostname R2901
aaa new-model
aaa authentication login SSLVPN local
!
crypto pki trustpoint RTR_AUTH
 enrollment selfsigned
 fqdn ciscoasa.vsb.cz
 subject-name CN=vsb.cz,CN=172.16.1.1
 revocation-check none
 rsakeypair RTR_AUTH
!
crypto pki certificate chain RTR_AUTH
username admin password 0 CqW87Fd
!
crypto vpn anyconnect flash0:/webvpn/anyconnectWIN_4.3.02039_k9.pkg sequence 1
!
interface GigabitEthernet0/0
 ip address 10.0.1.1 255.255.255.0
!
interface GigabitEthernet0/1
 ip address 172.16.1.1 255.255.255.0
!
ip local pool R2901_SSLVPN 10.0.1.3 10.0.1.100
ip forward-protocol nd
!
ip route 192.168.1.0 255.255.255.0 172.16.1.2
!
webvpn gateway R2901_GW1
 ip address 172.16.1.1 port 443
```

```
 http-redirect port 80
 ssl encryption aes128-sha1
 ssl trustpoint RTR_AUTH
 inservice
 !
webvpn context R2901_CONT1
 title "VSB-VPN"
 !
 acl "HOST_ACL"
   permit ip 192.168.1.0 255.255.255.0 10.0.1.0 255.255.255.0
 login-message "LOGIN IN SCHOOL WEBVPN"
 aaa authentication list SSLVPN
 gateway R2901_GW1
 max-users 15
 !
 ssl authenticate verify all
 !
 url-list "MyPages"
   heading "MyPages"
   url-text "WEB_SERVER" url-value "10.0.1.2"
 inservice
 !
 policy group R2901_POLICY1
   functions svc-enabled
   filter tunnel HOST_ACL
   svc address-pool "R2901_SSLVPN" netmask 255.255.255.224
   svc keep-client-installed
   svc rekey method new-tunnel
 default-group-policy R2901_POLICY1
!
end
```

Príloha H: *L2TP/IPSec VPN Cisco 2901 – skrátený výpis konfigurácie*

```
hostname L2TP
aaa new-model
aaa authentication ppp PPP_AUTH CqW87Fd
!
vpdn enable
!
vpdn-group L2TP
accept-dialin
protocol l2tp
virtual-template 1
no l2tp tunnel authentication
!
username cisco privilege 15 password 0 CqW87Fd
!
crypto isakmp policy 1
encr 3des
hash sha
authentication pre-share
group 2
lifetime 86400
!
crypto isakmp key Pda7M@9w4x address 0.0.0.0 0.0.0.0
!
crypto IPSec transform-set L2TP-Set2 esp-3des esp-sha-hmac
mode transport
!
crypto dynamic-map dyn-map 10
set transform-set L2TP_IPSEC
crypto dynamic-map dyn-map 10
```

```
crypto map L2TP_TUNNEL 65500 IPSec-isakmp dynamic dyn-map
!
crypto map outside_map
!
interface Virtual-Template1
ip unnumbered Loopback1
peer default ip address pool l2tp-pool
ppp authentication ms-chap-v2 VPDN_AUTH
!
ip local pool l2tp-pool 1.1.1.1 1.1.1.10
ip route 0.0.0.0 0.0.0.0 47.47.47.1
End
```

Príloha I: *Snímky obrazovky IPSec VPN*

```
R2TNL#sh crypto ikev2 sa det
 IPv4 Crypto IKEv2  SA

Tunnel-id Local                 Remote                fvrf/ivrf            Status
1         172.16.2.1/500        172.16.1.1/500        none/none            READY
      Encr: AES-CBC, keysize: 256, PRF: SHA256, Hash: SHA256, DH Grp:14, Auth sign: PSK, Auth verify:K
      Life/Active Time: 86400/55 sec
      CE id: 1007, Session-id: 7
      Status Description: Negotiation done
      Local spi: 6E01C53DCE1ACB50       Remote spi: CA36368901710CBE
      Local id: 172.16.2.1
      Remote id: 172.16.1.1
      Local req msg id:  2              Remote req msg id:  0
      Local next msg id: 2              Remote next msg id: 0
      Local req queued:  2              Remote req queued:  0
      Local window:      5              Remote window:      1
      DPD configured for 0 seconds, retry 0
      Fragmentation not configured.
      Extended Authentication not configured.
      NAT-T is not detected
      Cisco Trust Security SGT is disabled
      Initiator of SA : Yes
```

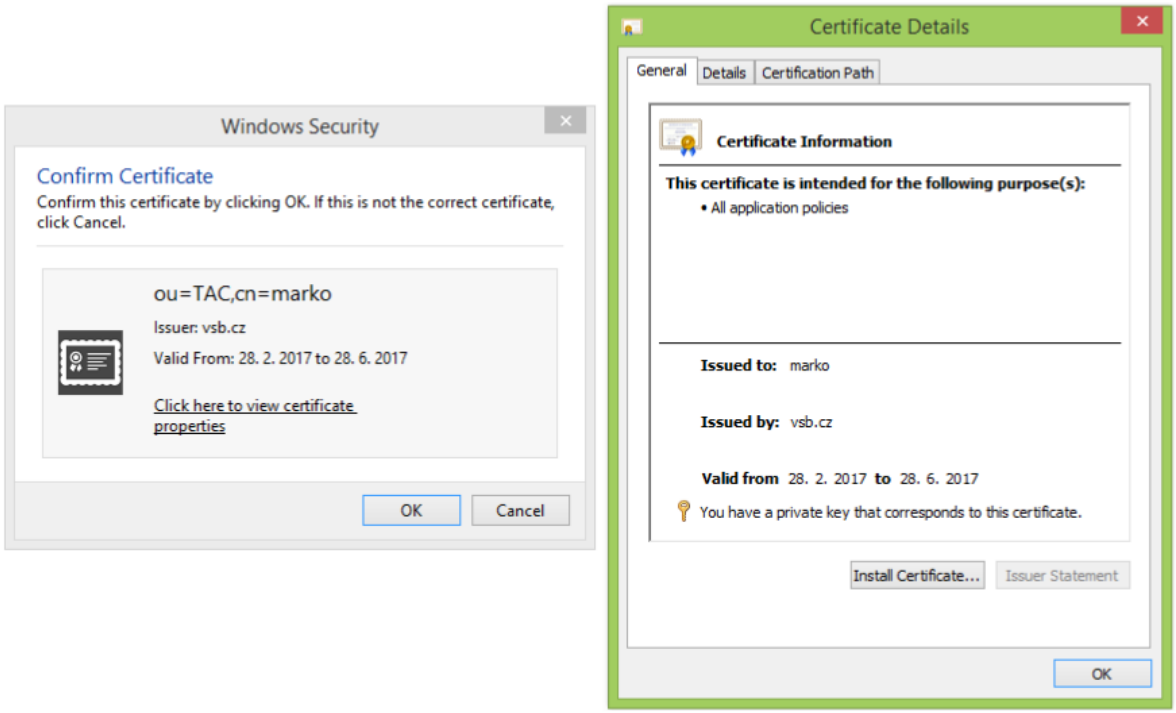
Smerovač Cisco 2901 IPSec VPN výpis ikev2 sa

```
R2TNL(config)#do sh crypto ipsec sa

interface: GigabitEthernet0/1
    Crypto map tag: IPsec, local addr 172.16.2.1

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (10.0.2.0/255.255.255.0/0/0)
   remote ident (addr/mask/prot/port): (10.0.1.0/255.255.255.0/0/0)
   current_peer 172.16.1.1 port 500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 59, #pkts encrypt: 59, #pkts digest: 59
    #pkts decaps: 8, #pkts decrypt: 8, #pkts verify: 8
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 0, #recv errors 0

     local crypto endpt.: 172.16.2.1, remote crypto endpt.: 172.16.1.1
     plaintext mtu 1438, path mtu 1500, ip mtu 1500, ip mtu idb GigabitEthernet0/1
     current outbound spi: 0xB2BF0C54(2998864980)
     PFS (Y/N): N, DH group: none

     inbound esp sas:
      spi: 0x9EA28D64(2661453156)
        transform: esp-192-aes esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 2004, flow_id: Onboard VPN:4, sibling_flags 80000040, crypto map: IPsec
        sa timing: remaining key lifetime (k/sec): (4160847/3504)
        IV size: 16 bytes
        replay detection support: Y
        Status: ACTIVE(ACTIVE)

     inbound ah sas:

     inbound pcp sas:

     outbound esp sas:
      spi: 0xB2BF0C54(2998864980)
        transform: esp-192-aes esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 2003, flow_id: Onboard VPN:3, sibling_flags 80000040, crypto map: IPsec
        sa timing: remaining key lifetime (k/sec): (4160839/3504)
        IV size: 16 bytes
        replay detection support: Y
        Status: ACTIVE(ACTIVE)
```

Smerovač Cisco 2901 IPSec VPN výpis IPSec sa

Príloha J: *Snímky obrazovky SSL VPN*

Prihlásenie sa pomocou mena a OTP Cisco ASA 5505



Autentifikácia užívateľa pomocou certifikátu Cisco ASA 5505

Príloha K: *Snímky obrazovky L2TP/IPSec VPN*

```
L2TP# sh crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id status
172.16.1.1      192.168.1.2     QM_IDLE           1009 ACTIVE

IPv6 Crypto ISAKMP SA
```

Prvá fáza ISAKMP SA Cisco 2901

```
L2TP#sh crypto ipsec sa

interface: GigabitEthernet0/1
    Crypto map tag: L2TP_TUNNEL, local addr 172.16.1.1

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (172.16.1.1/255.255.255.255/17/1701)
   remote ident (addr/mask/prot/port): (192.168.1.2/255.255.255.255/17/1701)
   current_peer 192.168.1.2 port 500
     PERMIT, flags={}
    #pkts encaps: 84, #pkts encrypt: 84, #pkts digest: 84
    #pkts decaps: 218, #pkts decrypt: 218, #pkts verify: 218
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 0, #recv errors 0

     local crypto endpt.: 172.16.1.1, remote crypto endpt.: 192.168.1.2
     plaintext mtu 1500, path mtu 1500, ip mtu 1500, ip mtu idb GigabitEthernet0/1
     current outbound spi: 0x0(0)
     PFS (Y/N): N, DH group: none

     inbound esp sas:

     inbound ah sas:

     inbound pcp sas:

     outbound esp sas:

     outbound ah sas:

     outbound pcp sas:

     local crypto endpt.: 172.16.1.1, remote crypto endpt.: 192.168.1.2
     plaintext mtu 1466, path mtu 1500, ip mtu 1500, ip mtu idb GigabitEthernet0/1
     current outbound spi: 0x8C9D3264(2359112292)
     PFS (Y/N): N, DH group: none

     inbound esp sas:
      spi: 0x5B59786E(1532590190)
        transform: esp-3des esp-sha-hmac ,
        in use settings ={Transport, }
        conn id: 2017, flow_id: Onboard VPN:17, sibling_flags 80000000, crypto map: L2TP_TUNNEL
        sa timing: remaining key lifetime (k/sec): (226898/3294)
        IV size: 8 bytes
        replay detection support: Y
        Status: ACTIVE(ACTIVE)
```

Druhá fáza IPSec SA Cisco 2901